目　　录

第一章 数学背景

要能够阅读本书，需要有比较全面的数学基础知识．许多不同的数学领域将在不同的章节发挥它们的作用．代数自然是最重要的，但读者还必须了解初等数论、概率论的一些事实以及组合论中的若干概念，诸如设计和几何．以下各节我们将扼要介绍一些预备知识，我们通常省略证明，想看证明的读者可参阅标准教科书．在某些章节，我们要用到关于一类不太为人熟知的正交多项式的大量事实，这类正交多项式叫做 Krawtchouk 多项式，它们的性质将在 § 1.2 中讨论．我们所用的记号都是很规范的，所以，在此仅提几个不十分熟知的．若 C 是一个有限集，我们用 $|C|$ 表示 C 中元素之个数；若表达式 B 是概念 A 的定义，则记 $A:=B$．单位矩阵和全 1 矩阵分别以 I 和 J 记之．类似地，分量全为 0(或 1)的向量简记为 $\mathbf{0}$(或 $\mathbf{1}$)．我们记 $\lfloor x\rfloor := \max\{n\in \mathbf{Z} \mid n\leqslant x\}$(注意，不是用 $[x]$)，而用符号 $\lceil x\rceil$ 表示 $\min\{n\in\mathbf{Z}\mid n\geqslant x\}$．

§ 1.1 代　　数

我们只需要少量初等数论知识．假定读者已经知道 N 中任何数都可以唯一写成素数之和(不计因子顺序)．若 a 整除 b，则我们记作 $a|b$．若 p 是一个素数，$p^r|a$，但 $p^{r+1}\nmid a$，则我们记作 $p^r\|a$．若 $k\in \mathbf{N}$，$k>1$，则 n 以 k 为基可以表示为

$$n=\sum_{i=0}^{l} n_i k^i,$$

对于每个 $0\leqslant i\leqslant l$，都有 $0\leqslant n_i<k$．既整除 a 又整除 b 的最大整数 n 称为 a 和 b 的最大公因子，记作 g.c.d(a, b) 或简记为 (a, b)．若 $m|a-b$，则我们记 $a\equiv b(\bmod m)$．

(1.1.1)定理. 若

$$\varphi(n) := |\{m \in \mathbb{N} \mid 1 \leqslant m \leqslant n, (m, n) = 1\}|,$$

则

(i) $\varphi(n) = n \prod_{p \mid n} (1 - 1/p)$,

(ii) $\sum_{d \mid n} \varphi(d) = n$.

函数 φ 称为 Euler 函数.

(1.1.2)定理. 若 $(a, m) = 1$, 则 $a^{\varphi(m)} \equiv 1 \pmod{m}$.

定理 1.1.2 称为 Euler-Fermat 定理.

(1.1.3)定义. Moebius 函数 μ 定义为

$$\mu(n) := \begin{cases} 1, & \text{若 } n = 1, \\ (-1)^k, & \text{若 } n \text{ 是 } k \text{ 个不同素因子之积}, \\ 0, & \text{其它}. \end{cases}$$

(1.1.4)定理. 若 f 和 g 都是定义在 $\mathbb{N}$ 上的函数，使得

$$g(n) = \sum_{d \mid n} f(d),$$

则

$$f(n) = \sum_{d \mid n} \mu(d) g\left(\frac{n}{d}\right).$$

定理 1.1.4 称为 Moebius 反演公式.

代数结构

我们假定读者熟悉线性代数的基本概念和定理，尽管有些我们在下面还会提及. 我们先给出一系列代数结构的定义，它们都是学习代数编码理论所必需的.

(1.1.5)定义. 一个群 $(G, \ )$ 是一个在其上定义了乘法运算的集合 G，满足

(i) $\forall_{a \in G} \forall_{b \in G} [ab \in G]$,

(ii) $\forall_{a \in G} \forall_{b \in G} \forall_{c \in G} [(ab)c = a(bc)]$,

(iii) $\exists_{e\in G}\forall_{a\in G}[ae = ea = a]$,

(元素 e 是唯一的),

(iv) $\forall_{a\in G}\exists_{b\in G}[ab = ba = e]$,

(b 称为 a 的逆元素,记作 a^{-1}).

进一步,若

(v) $\forall_{a\in G}\forall_{b\in G}[ab = ba]$,

则这个群叫做 Abel 群或交换群.

若 $(G, \ )$ 是群, $H\subset G$ 使得 $(H, \ )$ 也是一个群,则 $(H, \ )$ 叫做 $(G, \ )$ 的子群. 通常我们用 G 代替 $(G, \ )$. 一个有限群中元素的数目称为这个群的阶. 若 $(G, \ )$ 是群, $a\in G$, 那么,使得 $a^n = e$ 的最小正整数 n (如果存在的话)就称为 a 的阶. 在这种情况下,元素 $e, a, a^2, \cdots, a^{n-1}$ 构成一个以 a 为生成元的循环子群. 如果 $(G, \ )$ 是交换群, $(H, \ )$ 是一个子群,那么集合 $aH:=\{ah | h\in H\}$ 叫做 H 的陪集. 显然,两个陪集或者不交或者相等,所以这些陪集作成 G 的一个分划. 从陪集中选取的一个元素叫做这个陪集的代表元. 如果我们定义陪集乘法为 $(aH)(bH):=abH$, 则不难证明陪集构成一个群,这个群称为 G 的商群,记作 G/H. 由此我们注意到,若 $a\in G$, 则 a 的阶整除 G 的阶 (G 非 Abel 群亦然).

(1.1.6) 定义. 一个具有两种运算 (通常叫做加法和乘法)的集合 R, 记作 $(R, +, \ )$, 称为一个环, 如果

(i) $(R, +)$ 是一个 Abel 群,

(ii) $\forall_{a\in R}\forall_{b\in R}\forall_{c\in R}[(ab)c = a(bc)]$,

(iii) $\forall_{a\in R}\forall_{b\in R}\forall_{c\in R}[a(b+c) = ab + ac \wedge (a+b)c = ac + bc]$.

$(R, +)$ 的单位元通常记为 0.

若还具有性质

(iv) $\forall_{a\in R}\forall_{b\in R}[ab = ba]$,

则称这个环是交换环.

整数集 $\mathbf{Z}$ 是人们最熟悉的环的例子.

(1.1.7)定义. 设 $(R, +, \ )$是一个环，$\varnothing \neq S \subseteq R$，则 S 称为一个理想，如果

(i) $\forall_{a\in S}\forall_{b\in S}[ab\in S]$,

(ii) $\forall_{a\in S}\forall_{b\in R}[ab\in S \wedge ba\in S]$.

显然，如果 S 是 R 的理想，则$(S, +, \ )$是一个子环. 但条件(ii)比这个要强.

(1.1.8)定义. 域是一个环 $(R, +, \ )$，使得 $(R\backslash\{0\}, \ )$ 是一个 Abel 群.

(1.1.9)定理. 任何含有至少两个元素的有限环 R 是域，如果

$$\forall_{a\in R}\forall_{b\in R}[ab=0\Rightarrow(a=0\vee b=0)].$$

(1.1.10)定义. 设 $(V, +)$是一个 Abel 群，$\mathbf{F}$ 是一个域，定义 $\mathbf{F}\times V\to V$ 的乘法，满足

(i) $\forall_{\mathbf{a}\in V}[1\mathbf{a}=\mathbf{a}]$,

$\forall_{\alpha\in F}\forall_{\beta\in F}\forall_{\mathbf{a}\in V}[\alpha(\beta\mathbf{a})=(\alpha\beta)\mathbf{a}]$,

(ii) $\forall_{\alpha\in F}\forall_{\mathbf{a}\in V}\forall_{\mathbf{b}\in V}[\alpha(\mathbf{a}+\mathbf{b})=\alpha\mathbf{a}+\alpha\mathbf{b}]$,

$\forall_{\alpha\in F}\forall_{\beta\in F}\forall_{\mathbf{a}\in V}[(\alpha+\beta)\mathbf{a}=\alpha\mathbf{a}+\beta\mathbf{a}]$,

则三元组 $(V, +, \mathbf{F})$ 叫做域 $\mathbf{F}$ 上的一个向量空间. $(V, +)$的单位元记作 $\mathbf{0}$.

我们假定读者熟悉向量空间 $\mathbf{R}^n$，它由所有 n 元组$(a_1, a_2, \cdots, a_n)$构成，加法和乘法都是自然的. 我们提醒读者下列事实，即 $\mathbf{R}^n$ 的一个 k 维子空间 C 是这样一个向量空间，它有由向量 $\mathbf{a}_1:=(a_{11}, a_{12}, \cdots, a_{1n})$, $\mathbf{a}_2:=(a_{21}, a_{22}, \cdots, a_{2n})$, $\cdots$, $\mathbf{a}_k:=(a_{k1}, a_{k2}, \cdots, a_{kn})$ 组成的一组基. 这里基的意思是说，任意 $a\in C$ 都可以唯一写成 $\alpha_1\mathbf{a}_1+\alpha_2\mathbf{a}_2+\cdots+\alpha_k\mathbf{a}_k$. 读者还应熟悉用基向量的组合方法把一组基变到另一组的过程. 如前，我们通常把向量写成行向量. 两个向量 $\mathbf{a}$ 和 $\mathbf{b}$ 的内积 $\langle\mathbf{a}, \mathbf{b}\rangle$ 定义为

$$\langle\mathbf{a}, \mathbf{b}\rangle:=a_1b_1+a_2b_2+\cdots+a_nb_n.$$

一组基中的元素称为线性无关的. 换言之，这些向量的线性组合是 $\mathbf{0}$ 当且仅当所有系数为 0. 如果 $\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_k$ 是 k 个线性无关向量，即 k 维子空间 C 的一组基，那么方程组 $\langle\mathbf{a}_i, \mathbf{y}\rangle=0$ $(i=$

1, 2, ···, k) 以一个 $n-k$ 维子空间的所有向量为解. 我们把这个 $n-k$ 维子空间记作 $C^\perp$. 于是

$$C^\perp:=\{\mathbf{y}\in \mathbf{R}^n|\forall_{\mathbf{x}\in C}[\langle \mathbf{x}, \mathbf{y}\rangle=0]\}.$$

这些概念在后面起着基本的作用, 只是那里 R 将被一个有限域 F 所取代,但上述理论依然成立.

(1.1.11) 定义. 设 (V, +) 是 F 上一个向量空间, 并且定义了 $V\times V\to V$ 的乘法,满足

(i) (V, +,) 是一个环,

(ii) $\forall_{\alpha\in\mathbf{F}}\forall_{\mathbf{a}\in V}\forall_{\mathbf{b}\in V}[(\alpha\mathbf{a})\mathbf{b}=\mathbf{a}(\alpha\mathbf{b})]$,

则我们说这个系统是 F 上的一个代数.

设 (G, ·) 是一个有限群,我们把 G 的元素视为域 F 上某个向量空间 (V, +) 的一组基,那么 V 中元素可表为线性组合 $\alpha_1g_1+\alpha_2g_2+\cdots+\alpha_ng_n$, 其中

$$\alpha_i\in\mathbf{F},\ g_i\in G\ \ (1\leqslant i\leqslant n=|G|).$$

我们用显然的方式定义向量的乘法 *,即

$$\left(\sum_i\alpha_ig_i\right)*\left(\sum_j\beta_jg_j\right):=\sum_i\sum_j(\alpha_i\beta_j)(g_i\cdot g_j),$$

此式可写成 $\sum_k\gamma_kg_k$, 其中 γ_k 是所有使得 $g_ig_j=g_k$ 的对 (i, j) 所对应的 $\alpha_i\beta_j$ 之和. 这定义了一个代数,称之为 G 在 F 上的群代数,记为 **F**G.

例. 我们看几个与上面定义的概念有关的例子.

设 $A:=\{a_1, a_2, \cdots, a_n\}$ 是一个有限集,我们考虑所有 A 到 A 上的一一映射. 这些映射称为置换. 若 σ_1, σ_2 是置换, 我们定义 $\sigma_1\sigma_2$ 为 $(\sigma_1\sigma_2)(a):=\sigma_1(\sigma_2(a))$, 对所有 $a\in A$. 易见, A 上所有置换的集合 S_n 在该乘法下是一个群,叫做 n 次对称群. 在本书中,我们感兴趣的往往是特殊的置换群, 即 S_n 的子群. 我们举一个例子. 设 C 是 $\mathbf{R}^n$ 的 k 维子空间,考虑整数 1,2,···,n 的所有这样的置换 σ:若 $\mathbf{c}=(c_1, c_2, \cdots, c_n)\in C$, 则 $(c_{\sigma(1)}, c_{\sigma(2)}, \cdots, c_{\sigma(n)})$ 也在 C 中. 这些置换显然构成 S_n 的一个子群. 当然, C 常常使得

S_n 的这个子群仅含单位元. 但是有更有趣的例子! 另一个在下文中要出现的置换群例子是仿射置换群,其定义如下: 设 $\mathbf{F}$ 是一个(有限)域,映射 $f_{u,v}$, 其中 $u \in \mathbf{F}$, $v \in \mathbf{F}$, $u \neq 0$, 规定为 $f_{u,v}(x):= ux + v$, 对所有 $x \in \mathbf{F}$. 这些映射是 $\mathbf{F}$ 的置换, 它们关于函数的复合运算显然成群.

置换矩阵 P 是每行每列恰有一个 1 的 (0, 1)-矩阵. 我们说 P 对应于 $\{1, 2, \cdots, n\}$ 的置换 σ, 如果 $p_{ij} = 1$ 当且仅当 $i = \sigma(j)$ $(i = 1, 2, \cdots, n)$. 在这个约定之下, 置换之积对应于它们的矩阵之积. 由此,我们得到了所谓的置换群的矩阵表示.

一个作用在集合 Ω 上的置换群称为在 Ω 上是 k-传递的, 如果对 Ω 中任意两个相异元素的有序 k-元组 $(a_1, \cdots, a_k)$ 和 $(b_1, \cdots, b_k)$,都存在元素 $\sigma \in G$, 使得 $b_i = \sigma(a_i)$ $(1 \leqslant i \leqslant k)$. 如果 $k = 1$, 就说这个群是传递的.

设 S 是环 $(R, +, \ )$ 的理想, 因为 $(S, +)$ 是交换群 $(R, +)$的子群,所以我们可以作商群,陪集在这里叫做模 S 的剩余类. 对于这些类,我们引进一个显然的乘法: $(a + S)(b + S) := ab + S$. 不熟悉这一概念的读者最好验证该定义是有意义的 (即不依赖于代表元 a 和 b 的选取). 这样, 我们构造了一个环,叫做 R 模 S 的剩余类环,并记作 R/S. 下面的例子读者一定是熟悉的.设 $R := \mathbf{Z}$, p 是素数, 令 S 是 p 的所有倍数组成的集合 $p\mathbf{Z}$ (有时也记为(p)). 那么, R/S 就是整数模 p 的环. R/S 的元素可以表为 $0, 1, \cdots, p-1$, 而加法和乘法则是在 $\mathbf{Z}$ 中作通常运算后再用 p 模. 例如取 $p = 7$, 则 $4+5 = 2$,因为在 $\mathbf{Z}$ 中, $4+5 \equiv 2 \pmod 7$. 同理, 在 $\mathbf{Z}/7\mathbf{Z} = \mathbf{Z}/(7)$ 中, $4 \cdot 5 = 6$. 若 S 是 $\mathbf{Z}$ 的理想, $S \neq \{0\}$, 则存在最小正整数 $k \in S$. 设 $s \in S$, 我们可以把 s 写成 $ak + b$ 的形式, 其中 $0 \leqslant b < k$. 由理想的定义我们有 $ak \in S$, 所以 $b = s - ak \in S$, 从而由 k 的定义知 $b = 0$. 因此 $S = (k)$. 由一个固定元素的所有倍数组成的理想称为主理想, 如果一个 R 除子理想外没有其它理想, 则称为主理想环. 由此即知 $\mathbf{Z}$ 是一个主理想环.

(1.1.12) 定理. 若 p 是素数,则 $\mathbf{Z}/p\mathbf{Z}$ 是域.

这是定理 1.1.9 的直接推论,但是直接验证也很显然. n 个元素的有限域记为 $\mathbf{F}_n$ 或 $GF(n)$ (Galois 域).

环和有限域

我们将在下面对有限域作较多的讨论. 首先讨论环与理想. 设 $\mathbf{F}$ 是一个有限域. 考虑由全体多项式 $a_0 + a_1x + \cdots + a_nx^n$ 组成的集合 $\mathbf{F}[x]$, 其中 n 可以是 $\mathbf{N}$ 中任何数, $a_i \in \mathbf{F}$, $0 \leqslant i \leqslant n$. 在通常的多项式加法和乘法的定义下, 它构成一个环 $(\mathbf{F}[x], +, \ )$,这个环一般就记为 $\mathbf{F}[x]$. 某个多项式 $g(x)$ 的所有倍式, 即形如 $a(x)g(x)$, $a(x) \in \mathbf{F}[x]$ 的多项式组成的集合是 $\mathbf{F}[x]$ 的理想. 和前一样,这个理想记为 $(g(x))$. 下述定理表明 $\mathbf{F}[x]$ 中没有其它类型的理想.

(1.1.13) 定理. $\mathbf{F}[x]$ 是主理想环.

剩余类环 $\mathbf{F}[x]/(g(x))$ 可由小于 $g(x)$ 次数的多项式来表示. 如同上面举的例子 $\mathbf{Z}/7\mathbf{Z}$, 我们先对代表元作通常的加法与乘法, 然后用 $g(x)$ 模. 例如,取 $\mathbf{F} = \mathbf{F}_2 = \{0, 1\}$, $g(x) = x^3 + x + 1$, 那么 $(x + 1)(x^2 + 1) = x^3 + x^2 + x + 1 = x^2$. 对于不熟悉有限域的读者来说, 仔细研究一下这个例子是有益的. 首先注意到 $g(x)$ 是不可约的,即不存在次数小于 3 的多项式 $a(x)$ 和 $b(x) \in \mathbf{F}[x]$, 使得 $g(x) = a(x)b(x)$. 其次,我们看到,上述性质意味着在 $\mathbf{F}_2[x]/(g(x))$ 中, 两个元素 $a(x)$ 和 $b(x)$ 之积为零当且仅当 $a(x) = 0$ 或 $b(x) = 0$. 由定理 1.1.9, $\mathbf{F}_2[x]/(g(x))$ 是域. 因为这个剩余类环的代表元的次数都小于 3, 所以恰有 8 个元素.这样, 我们找到了一个含有 8 个元素的域,即 $\mathbf{F}_{2^3}$. 这个例子给出了构造有限域的方法.

(1.1.14) 定理. 设 p 是一个素数, $g(x)$ 是环 $\mathbf{F}_p[x]$ 的一个 r 次不可约多项式,则剩余类环 $\mathbf{F}_p[x]/(g(x))$ 是 p^r 个元素的有限域.

证明. 证明与所给的 $p = 2$, $r = 3$, $g(x) = x^3 + x + 1$ 的例子一样. □

(1.1.15) 定理. 设 $\mathbf{F}$ 是 n 个元素的域，则 n 是素数的方幂.

证明. 由定义,$\mathbf{F}$ 关于乘法有一个单位元，记为 1. 当然 $1+1 \in \mathbf{F}$，这个元我们记为 2. 依次类推，即 $2+1=3$ 等等. 经有限次后，我们会遇到一个已经有"记号"的域中元素. 假如说 k 个 1 之和等于 l 个 1 之和 $(k>l)$，那么，$(k-l)$ 个 1 之和就是 0，即我们第一次遇到了已经有记号的元素，这个元素就是 0. 设 0 是 k 个 1 之和. 如果 k 是合数，$k=ab$，则我们分别称之为 a 和 b 的这两个元素之积为 0，矛盾. 所以 k 是素数. 这证明 $\mathbf{F}_p$ 是 $\mathbf{F}$ 的一个子域. 我们用显然的方式定义 $\mathbf{F}$ 中一个元素集关于（系数取自）$\mathbf{F}_p$ 的线性无关性. 设在所有线性无关子集中，$\{x_1, x_2, \cdots, x_r\}$ 是元素个数是最多的. 若 $x \in \mathbf{F}$，则 $x, x_1, x_2, \cdots, x_r$ 是线性相关的，也就是说，存在系数 $0 \neq \alpha, \alpha_1, \cdots, \alpha_r$ 使得 $\alpha x+\alpha_1 x_1+\cdots+\alpha_r x_r=0$. 因此，$x$ 是 x_1 到 x_r 的一个线性组合. 因为显然有 p^r 个 x_1 到 x_r 的不同的线性组合，所以即得我们的结论. □

如果我们能证明，对于任意 $r \geqslant 1$，$\mathbf{F}_p[x]$ 中存在 r 次不可约多项式，那么，由上述定理可知，n 个元素的域存在当且仅当 n 是素数的幂. 下面我们通过计算这种多项式的个数来证明 r 次不可约多项式的存在性. 固定 p，并以 I_r 表示 r 次首一（即 x^r 的系数为 1）不可约多项式的个数. 我们断言

$$(1.1.16) \qquad (1-pz)^{-1}=\prod_{r=1}^{\infty}(1-z^r)^{-I_r}.$$

欲证此式，首先注意到左边 z^n 的系数是 p^n，它是系数在 $\mathbf{F}_p$ 中的 n 次首一多项式的个数. 我们知道，每一个这样的多项式都可唯一地分解为不可约因子的乘积，因此，我们必须确信这些乘积都计算在(1.1.16)的右边了. 要证明这点，只需考虑两个次数分别为 r 和 s 的不可约多项式 $a_1(x)$ 和 $a_2(x)$. 乘积 $(a_1(x))^k(a_2(x))^l$ 与 $(1+z_1^r+z_1^{2r}+\cdots)$ 和 $(1+z_2^s+z_2^{2s}+\cdots)$ 的乘积中的项 $z_1^{kr}z_2^{ls}$ 有一个一一对应. 如果 z_1 和 z_2 都恒同于 z，那么 z 的指数就是 $(a_1(x))^k(a_2(x))^l$ 的次数. 考虑所有不可约多项式而不是两个多项式 $a_1(x)$ 和 $a_2(x)$，则我们即得(1.1.16).

在(1.1.16)两边取对数，然后微分，最后同乘以 z，得到

(1.1.17) $$\frac{pz}{1-pz}=\sum_{r=1}^{\infty}I_r\frac{rz^r}{1-z^r}.$$

比较(1.1.17)两边 z^n 的系数，我们发现

(1.1.18) $$p^n=\sum_{r\mid n}rI_r.$$

对 (1.1.18) 应用定理 1.1.4 得

(1.1.19) $$I_r=\frac{1}{r}\sum_{d\mid r}\mu(d)p^{r/d}>\frac{1}{r}\{p^r-p^{r/2}-p^{r/3}-\cdots\}$$

$$>\frac{1}{r}\left(p^r-\sum_{i=0}^{r/2}p^i\right)>\frac{1}{r}p^r(1-p^{-\frac{r}{2}+1})>0.$$

既然我们现在知道了对哪些 n 值存在 n 元域，我们自然希望了解这些域的更多的性质. $\mathbf{F}_{p^r}$ 的结构在本书的许多章节起着十分重要的作用. 作为准备，我们考虑有限域 $\mathbf{F}$ 和一个多项式 $f(x)\in\mathbf{F}[x]$，使得 $f(a)=0$，其中 $a\in\mathbf{F}$. 那么通过做除法可知，存在 $g(x)\in\mathbf{F}[x]$，使得 $f(x)=(x-a)g(x)$. 依次往下做，我们得到一个简单事实，即 $\mathbf{F}[x]$ 中 r 次多项式在 $\mathbf{F}[x]$ 中至多有 r 个零点.

如果 α 是乘法群 $(\mathbf{F}_{p^r}\backslash\{0\},\ )$ 的一个 e 阶元素，那么 α 是多项式 x^e-1 的零点. 事实上我们有

$$x^e-1=(x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{e-1}).$$

因此该群中仅有的 e 阶元是 α^i，其中 $1\leqslant i<e$ 且 $(i,e)=1$.这种元素共有 $\varphi(e)$ 个. 所以对每个整除 p^r-1 的 e，域中的 e 阶元素或者是 0 个，或者是 $\varphi(e)$ 个. 但由 (1.1.1) 知不可能出现 0 个. 由此推得存在 p^r-1 阶元素. 实际上恰有 $\varphi(p^r-1)$ 个 p^r-1 阶元素. 我们已经证明了下列定理.

(1.1.20) 定理. 在 $\mathbf{F}_q$ 中，乘法群 $(\mathbf{F}_q\backslash\{0\},\ )$是循环群.

这个群常常记为 $\mathbf{F}_q^*$.

(1.1.21) 定义. $\mathbf{F}_q$ 的乘法群的生成元称为这个域的本原元.

定理 1.1.20 表明 $\mathbf{F}_q$ 的元素恰是多项式 x^q-x 的 q 个不同零

点．使得 $\beta^k=1$，而 $\beta^l\neq 1$，对于 $0<l<k$ 的元素 β 叫做 k 次本原单位根．显然 $\mathbf{F}_q$ 的本原元 α 是 $(q-1)$ 次本原单位根．如果 e 整除 $q-1$，那么 α^e 是 $(q-1)/e$ 次本原单位根．进一步，定理 1.1.20 的一个推论是，$\mathbf{F}_{p^r}$ 是 $\mathbf{F}_{p^s}$ 的一个子域当且仅当 r 整除 s．实际上这个叙述可能会使读者感到有点含混不清，因为我们所用的符号暗示了，对于给定的 q，$\mathbf{F}_q$ 是唯一的．这的确是对的．事实上，这可以从(1.1.18)得到．我们已经证明对于 $q=p^n$，$\mathbf{F}_q$ 中任意元都是 x^q-x 的某个不可约因子的零点，又由上面的说明和定理 1.1.14 我们看到，这个因子的次数 r 整除 n．由(1.1.18)这意味着我们用到了所有 r 次不可约多项式，其中 $r|n$，换句话说，这些多项式之积就是 x^q-x．这证明了两个阶为 q 的域 $\mathbf{F}$ 和 $\mathbf{F}'$ 是同构的，即存在一一映射 $\varphi:\mathbf{F}\to\mathbf{F}'$ 保持加法和乘法．

下述定理在本书中经常用到．

(1.1.22) 定理． 设 $q=p^r$，$0\neq f(x)\in\mathbf{F}_q[x]$．

(i) 若 $\alpha\in\mathbf{F}_{q^k}$ 且 $f(\alpha)=0$，则 $f(\alpha^q)=0$．

(ii) 反之，若对于任意使得 $f(\alpha)=0$ 的 α 都有 $f(\alpha^q)=0$，则 $f(x)\in\mathbf{F}_q[x]$．

证明．(i) 由于 p 整除 $\binom{p}{k}$，$1\leqslant k\leqslant p-1$，由二项式定理我们有 $(a+b)^p=a^p+b^p$．由此得 $(a+b)^q=a^q+b^q$．如果 $f(x)=\sum a_ix^i$，则 $(f(x))^q=\sum a_i^q(x^q)^i$．因为 $a_i\in\mathbf{F}_q$，所以 $a_i^q=a_i$．代入 $x=\alpha$ 得 $f(\alpha^q)=(f(\alpha))^q=0$．

(iii) 我们已经知道在 $\mathbf{F}_q$ 的一个适当的扩域中，多项式 $f(x)$ 是因子 $x-\alpha_i$ 的乘积(即都是 1 次的)，且如果 $x-\alpha_i$ 是其中一个因子，那么 $x-\alpha_i^q$ 也是其中一个因子．设 $f(x)=\sum_{k=0}^{n}a_kx^k$，则 a_k 是零点 α_i 的对称函数，因此 $a_k=a_k^q$，也就是 $a_k\in\mathbf{F}_q$．□

若 $\alpha\in\mathbf{F}_q$，$q=p^r$，那么 α 在 $\mathbf{F}_q$ 上的极小多项式是使得 $f(\alpha)=0$ 的不可约多项式 $f(x)\in\mathbf{F}_q[x]$．若 α 的阶为 e，则由定理 1.1.22 知，其极小多项式就是

$$\prod_{i=0}^{m-1}(x-\alpha^{q^i}),$$

其中m是使得 $q^m\equiv 1(\bmod e)$ 的最小正整数．有时，我们要考虑固定一个本原元α的域$\mathbf{F}_q$．

在这种情况下，我们用 $m_i(x)$ 来记α^i的极小多项式．一个不可约多项式称为本原多项式，如果它是相应域中一个本原元的极小多项式．这种多项式在定理 1.1.14 的构造中用起来最方便．我们详细举一个例子．

(1.1.23)例．多项式 x^4+x+1 在$\mathbf{F}_2$上是本原的．域$\mathbf{F}_{2^4}$由次数<4的多项式表示．多项式x是一个本原元．因为我们更习惯于在其它场合使用符号x，所以我们称这个本原元为α． 注意到 $\alpha^4+\alpha+1=0$，每个$\mathbf{F}_{2^4}$中的元素都是$1,\alpha,\alpha^2,\alpha^3$的线性组合．我们得到下列$\mathbf{F}_{2^4}$的表．读者可以看出这跟域R的对数表是对等的．

$\mathbf{F}_{2^4}$ 的表

$0=$		$=(0\ 0\ 0\ 0)$
$1=$	1	$=(1\ 0\ 0\ 0)$
$\alpha=$	α	$=(0\ 1\ 0\ 0)$
$\alpha^2=$	α^2	$=(0\ 0\ 1\ 0)$
$\alpha^3=$	α^3	$=(0\ 0\ 0\ 1)$
$\alpha^4=$	$1+\alpha$	$=(1\ 1\ 0\ 0)$
$\alpha^5=$	$\alpha+\alpha^2$	$=(0\ 1\ 1\ 0)$
$\alpha^6=$	$\alpha^2+\alpha^3$	$=(0\ 0\ 1\ 1)$
$\alpha^7=$	$1+\alpha+\alpha^3$	$=(1\ 1\ 0\ 1)$
$\alpha^8=$	$1+\alpha^2$	$=(1\ 0\ 1\ 0)$
$\alpha^9=$	$\alpha+\alpha^3$	$=(0\ 1\ 0\ 1)$
$\alpha^{10}=$	$1+\alpha+\alpha^2$	$=(1\ 1\ 1\ 0)$
$\alpha^{11}=$	$\alpha+\alpha^2+\alpha^3$	$=(0\ 1\ 1\ 1)$
$\alpha^{12}=$	$1+\alpha+\alpha^2+\alpha^3$	$=(1\ 1\ 1\ 1)$
$\alpha^{13}=$	$1+\alpha^2+\alpha^3$	$=(1\ 0\ 1\ 1)$
$\alpha^{14}=$	$1+\alpha^3$	$=(1\ 0\ 0\ 1)$

右边的表示再次表明$\mathbf{F}_{2^4}$可以看成是向量空间$(\mathbf{F}_2)^4$，其中

$\{1, \alpha, \alpha^2, \alpha^3\}$ 是一组基．左边一列作乘法最容易（指数相加，mod15），而右边一列作加法最容易(向量相加)．容易验证

$$m_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$$
$$= x^4 + x + 1,$$
$$m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$$
$$= x^4 + x^3 + x^2 + x + 1,$$
$$m_5(x) = (x-\alpha^5)(x-\alpha^{10}) = x^2 + x + 1,$$
$$m_7(x) = (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})$$
$$= x^4 + x^3 + 1,$$

又，$x^{16} - x$ 的不可约分解是

$$x^{16} - x = x(x-1)(x^2+x+1)(x^4+x+1)$$
$$\cdot (x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

注意 $x^4 - x = x(x-1)(x^2+x+1)$ 对应于元素 $0, 1, \alpha^5, \alpha^{10}$，它们组成子域 $\mathbf{F}_4 = \mathbf{F}_2[x]/(x^2+x+1)$．多项式 $m_3(x)$ 不可约，但非本原．

不熟悉有限域的读者应把 (1.1.14)至(1.1.23) 学习透，并构造几个例子，如 $\mathbf{F}_9$, $\mathbf{F}_{27}$, $\mathbf{F}_{64}$，以及相应的极小多项式、子域等等．有限域的表可查阅参考文献 [9] 和[10]．

多项式

我们还需要一些关于多项式的事实．若 $f(x) \in \mathbf{F}_q[x]$，则我们可以纯形式地定义**导数** $f'(x)$ 为

$$\left(\sum_{k=0}^{n} a_k x^k\right)' := \sum_{k=1}^{n} k a_k x^{k-1}.$$

有关和与积的导数的通常规则都是可行的．例如 $(x-\alpha)^2 f(x)$的导数是 $2(x-\alpha)f(x) + (x-\alpha)^2 f'(x)$．因此，下述定理是显而易见的．

(1.1.24) 定理． *若 $f(x) \in \mathbf{F}_q[x]$，α 是 $f(x)$ 在 $\mathbf{F}_q$ 的某个扩域里的重零点，则 α 仍是导数 $f'(x)$ 的零点．*

后面要用到的另一个结论是，若

$$f(x)=\prod_{i=1}^{n}(x-\alpha_i),$$

则

$$f'(x)=\sum_{i=1}^{n}f(x)/(x-\alpha_i).$$

下述定理是众所周知的.

(1.1.25) 定理. 若多项式 $a(x)$ 和 $b(x)\in \mathbf{F}[x]$ 的最大公因子是 1，则在 $\mathbf{F}[x]$ 中存在多项式 $p(x)$ 和 $q(x)$ 使得

$$a(x)p(x)+b(x)q(x)=1.$$

证明. 这是定理 1.1.13 的直接推论. □

虽然我们由 (1.1.19) 知道，任意次数 r 的不可约多项式存在，但是真要找到一个有时需做大量工作. (1.1.19) 的证明提供了一种方法. 我们可以从所有可能的一次多项式出发，用它们构造所有 2 次可约多项式. 任何不在其中的 2 次多项式都是不可约的. 继续用这个办法显然可产生 3 次不可约多项式，等等. 在 § 9.2 我们要用到 $\mathbf{F}_2$ 上任意高次数的不可约多项式，上述方法不能满足这个要求. 因而我们给出如下方法.

(1.1.26)引理.

$$3^{\beta+1}\|(2^{3^\beta}+1).$$

证明. (i) 对于 $\beta=0$ 和 $\beta=1$，结论成立.

(ii) 设 $3^t\|(2^{3^\beta}+1)$. 那么由

$$(2^{3^{(\beta+1)}}+1)=(2^{3^\beta}+1)\{(2^{3^\beta}+1)(2^{3^\beta}-2)+3\},$$

即知，若 $t\geqslant 2$，则 $3^{t+1}\|(2^{3^{(\beta+1)}}+1)$. □

(1.1.27) 引理. 若 $2(\mathrm{mod}\ 3^l)$ 的阶为 m，则

$$m=\varphi(3^l)=2\cdot 3^{l-1}.$$

证明. 若 $2^\alpha\equiv 1(\mathrm{mod}\ 3)$，则 α 是偶数. 因此 $m=2s$，从而 $2^s+1\equiv 0(\mathrm{mod}\ 3^l)$. 再由定理 1.1.2 和引理 1.1.26 即得结论. □

(1.1.28) 定理. 设 $m=2\cdot 3^{l-1}$，则

$$x^m+x^{m/2}+1$$

在 $\mathbf{F}_2$ 上不可约.

证明．考虑 $\mathbf{F}_{2^m}$．设 ξ 是这个域中的一个 3^l 次本原单位根．由引理 1.1.27，ξ 的极小多项式是一个 m 次多项式

$$f(x)=(x-\xi)(x-\xi^2)(x-\xi^4)\cdots(x-\xi^{2^{m-1}}).$$

注意到

$$x^{3^l}+1=(1+x)(1+x+x^2)(1+x^3+x^6)\cdots(1+x^{3^{l-1}}+x^{2\cdot 3^{l-1}}),$$

此分解式中只有一个 m 次多项式，所以最后的因子必定是 $f(x)$，即 $f(x)$ 是不可约的． □

二次剩余

任意域 $\mathbf{F}_q$ 中本原元的存在性使得在域中确定平方元很容易．如果 q 是偶数，那么每个元素都是平方元．如果 q 是奇数，那么 $\mathbf{F}_q$ 含 $\frac{1}{2}(q-1)$ 个非零平方元和 $\frac{1}{2}(q-1)$ 个非平方元． 在 $\mathbf{F}_p$ 中是平方的那些整数 $k(1\leqslant k\leqslant p-1)$ 通常称为模 p 的**二次剩余**．把 $k\in\mathbf{F}_p$ 写成这个域中一个本原元的方幂，我们看到 k 是二次剩余当且仅当 $k^{(p-1)/2}\equiv 1\pmod p$．对于元素 $p-1=-1$，我们发现 -1 在 $\mathbf{F}_p$ 中是平方元当且仅当 $p\equiv 1(\bmod 4)$．在 § 6.9 我们需要知道 2 在 $\mathbf{F}_p$ 中是否为平方元．为解决这个问题，我们考虑元素 $1,2,\cdots,(p-1)/2$，并设 a 是它们的乘积．用 2 乘每个元素得到 $2,4,\cdots,p-1$，这个序列中的 $\left\lfloor\frac{p-1}{4}\right\rfloor$ 个项是 a 的因子，而对于 a 的任何其它因子 k，$-k$ 是大于 $\frac{(p-1)}{2}$ 的偶数．由此在 $\mathbf{F}_p$ 中我们有 $2^{(p-1)/2}a=(-1)^{(p-1)/2-\lfloor(p-1)/4\rfloor}a$．因为 $a\neq 0$，所以 2 是平方元当且仅当

$$\frac{p-1}{2}-\left\lfloor\frac{p-1}{4}\right\rfloor$$

是偶数，即 $p\equiv\pm 1\pmod 8$．

迹

设 $q=p^r$，定义映射 $\mathrm{Tr}:\mathbf{F}_q\to\mathbf{F}_p$ 如下

(1.1.29) 定义. 若 $\xi \in \mathbf{F}_q$，则

$$\mathrm{Tr}(\xi) := \xi + \xi^p + \xi^{p^2} + \cdots + \xi^{p^{r-1}}$$

称为迹(函数).

(1.1.30) 定理. 迹函数有如下性质:

(i) 对任何 $\xi \in \mathbf{F}_q$，迹 $\mathrm{Tr}(\xi)$ 在 $\mathbf{F}_p$ 中;

(ii) 存在元素 $\xi \in \mathbf{F}_q$，使得 $\mathrm{Tr}(\xi) \neq 0$;

(iii) Tr 是线性映射.

证明. (i) 由定义，$(\mathrm{Tr}(\xi))^p = \mathrm{Tr}(\xi)$.

(ii) 方程 $x + x^p + \cdots + x^{p^{r-1}} = 0$ 在 $\mathbf{F}_q$ 中不可能有 q 个根.

(iii) 因为 $(\xi + \eta)^p = \xi^p + \eta^p$，且对每个 $a \in \mathbf{F}_p$ 都有 $a_p = a$，所以结论显然成立. □

很明显，定理蕴含: 迹函数取到每个值 $p^{-1}q$ 次，而且多项式 $x + x^p + \cdots + x^{p^{r-1}}$ 是极小多项式的一个乘积（试就例 1.1.23 验证这一结论).

特征标

设$(G, +)$是一个群，又设$(T, \quad)$是绝对值为 1 的复数群，运算为乘法. 特征标是一个同态 $\chi: G \to T$，即

(1.1.31) $\quad \forall_{g_1 \in G} \forall_{g_2 \in G} [\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)]$.

由定义可知，对任何特征标都有 $\chi(0) = 1$. 如果对所有 $g \in G$ 都有 $\chi(g) = 1$，则称 χ 为主特征标.

(1.1.32) 引理. 若 χ 是 $(G, +)$ 的特征标，则

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{若 } \chi \text{ 是主特征标}, \\ 0, & \text{其它}. \end{cases}$$

证明. 设 $h \in G$，则

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(h + g) = \sum_{k \in G} \chi(k).$$

若 χ 不是主特征标，则我们可选取 h，使得 $\chi(h) \neq 1$. □

§1.2 Krawtchouk 多项式

在这一节中，我们要介绍一类在编码理论若干分支中起着重要作用的多项式，即 Krawtchouk 多项式. 这些多项式是正交多项式的实例. 我们所提到的定理，大部分都是对于任何正交多项式序列成立的一般定理的特殊情形. 我们建议不了解分析中这一十分精彩部分的读者去查阅一本有关正交多项式的教科书（例如 G. Szegö [67], D.Jackson [36], F.G. Tricomi [70]）. 事实上，在下面提到的定理当中，就有一些证明是留待读者去查阅有关文献的. 由于这些多项式在下文中至为重要，我们要对其作较这个引言的其它内容更广泛的讨论.

Krawtchouk 多项式通常出现在两个参数 n 和 q 已经固定的情形,所以在这些多项式的符号中往往省略.

(1.2.1)定义. 对于 $k=0,1,2,\cdots$,我们定义 Krawtchouk **多项式** $K_k(x)$ 为

$$K_k(x;n,q):=K_k(x):=\sum_{j=0}^{k}(-1)^j\binom{x}{j}\binom{n-x}{k-j}(q-1)^{k-j},$$

其中

$$\binom{x}{j}:=\frac{x(x-1)\cdots(x-j+1)}{j!},\quad (x\in\mathrm{R}).$$

考察 $q=2$ 的特殊情形,我们有

$$(1.2.2)\quad K_k(x)=\sum_{j=0}^{k}(-1)^j\binom{x}{j}\binom{n-x}{k-j}=(-1)^kK_k(n-x).$$

作 $(1+(q-1)z)^{n-x}$ 和 $(1-z)^x$ 的 Taylor 级数的乘积,得

$$(1.2.3)\quad \sum_{k=0}^{\infty}K_k(x)z^k=(1+(q-1)z)^{n-x}(1-z)^x.$$

由(1.2.1) 显然可知，$K_k(x)$ 是 x 的 k 次多项式，首项系数为 $(-q)^k/k!$. 之所以称它们为正交多项式，是因为它们有下列的"正交关系"：

(1.2.4) $$\sum_{i=0}^{n}\binom{n}{i}(q-1)^{i}K_{k}(i)K_{l}(i)=\delta_{kl}\binom{n}{k}(q-1)^{k}q^{n}.$$

读者容易证明这个关系式，这只要在上式两边同乘 $x^{k}y^{l}$，然后对 k 和 l 作和（从 0 到∞），再利用(1.2.3). 因为两个和式相等，所以结论为真. 由(1.2.1)得

(1.2.5) $$(q-1)^{i}\binom{n}{i}K_{k}(i)=(q-1)^{k}\binom{n}{k}K_{i}(k),$$

代入(1.2.4)，我们得到第二个正交关系：

(1.2.6) $$\sum_{i=0}^{n}K_{l}(i)K_{i}(k)=\delta_{lk}q^{n}.$$

我们列举几个 Krawtchouk 多项式 ($k\leqslant 2$)，

(1.2.7)
$$K_{0}(n,x)=1,$$
$$K_{1}(n,x)=n(q-1)-qx,\ (=n-2x \text{ 若 } q=2),$$
$$K_{2}(n,x)=\frac{1}{2}\{q^{2}x^{2}-q(2qn-q-2n+2)x+(q-1)^{2}n(n-1)\},$$
$$\left(=2x^{2}-2nx+\binom{n}{2}\text{若 } q=2\right).$$

在第七章，我们要用到 $K_{k}(x)$ 表达式中 x^{k}，x^{k-1}，x^{k-2} 以及 x^{0} 的系数. 假设 $K_{k}(x)=\sum_{i=0}^{k}c_{i}x^{i}$，那么对于 $q=2$ 我们有

(1.2.8)
$$c_{k}=(-2)^{k}/k!,$$
$$c_{k-1}=(-2)^{k-1}n/(k-1)!,$$
$$c_{k-2}=\frac{1}{6}(-2)^{k-2}\{3n^{2}-3n+2k-4\}/(k-2)!,$$
$$c_{0}=\sum_{j=0}^{k}(-1)^{j}\binom{n}{k-j}.$$ [1]

有时我们还需要 Krawtchouk 多项式的某些递归关系. 最重要的

---

1) 这最后一个表达式是译者加的. ——译者注

一个是

(1.2.9) $$(k+1)K_{k+1}(x)=\{k+(q-1)(n-k)-qx\}\cdot K_k(x)-(q-1)(n-k+1)K_{k-1}(x).$$

这是容易证明的;我们在(1.2.3)的两边对 z 微分,并乘以 $(1+(q-1)z)(1-z)$. 比较系数即得结论. 一个更简单的练习是在(1.2.3)中以 $x-1$ 代替 x 而得到

(1.2.10) $$K_k(i)=K_k(i-1)-(q-1)K_{k-1}(i)-K_{k-1}(i-1),$$

利用此式递归地计算 $K_k(i)$ 很方便.

设 $P(x)$ 是一个 l 次多项式，则存在唯一的展开式

(1.2.11) $$P(x)=\sum_{k=0}^{l}\alpha_k K_k(x),$$

称之为 $P(x)$ 的 Krawtchouk **展开式**

我们不加证明地给出若干以后要用的性质，它们都是正交多项式的一般定理的特殊情形. 首先是 Christoffel-Darboux 公式

(1.2.12) $$\frac{K_{k+1}(x)K_k(y)-K_k(x)K_{k+1}(y)}{y-x}=\frac{2}{k+1}\binom{n}{k}\sum_{i=0}^{k}\frac{K_i(x)K_i(y)}{\binom{n}{i}}.$$

利用递归关系(1.2.9)和归纳法,可以得到十分重要的 $K_k(x)$ 零点的交错性质:

(1.2.13) $K_k(x)$ 在 $(0, n)$ 内有 k 个实零点；若它们是 $v_1<v_2<\cdots<v_k$, 而且 $u_1<u_2<\cdots<u_{k-1}$ 是 $K_{k-1}(x)$ 的零点,则

$$0<v_1<u_1<v_2<\cdots<v_{k-1}<u_{k-1}<v_k<n.$$

下述性质还是由 (1.2.3) 经两个级数相乘得到(我们取 $q=2$): 若 $x=0, 1, 2, \cdots, n$, 则

(1.2.14) $$K_i(x)K_j(x)=\sum_{k=0}^{n}\alpha_k K_k(x),$$

其中

$$\alpha_k := \binom{n-k}{(i+j-k)/2}\binom{k}{(i-j+k)/2}.$$

在第七章我们需要关系式:

(1.2.15) $$\sum_{k=0}^{l} K_k(x) = K_l(x-1;\ n-1,\ q).$$

替换(1.2.1)的左端,改变求和顺序,然后利用

$$\binom{x}{j} = \binom{x-1}{j-1} + \binom{x-1}{j}\ (j \geqslant 1),$$

即证得上式. 我们把 $K_l(x-1; n-1, q)$ 记作 $\Psi_l(x)$.

§1.3 组 合 论

在若干章节中,我们要使用组合论的概念和结论. 这一节我们仅回顾一些定义和一个定理. 不熟悉这一数学领域的读者可参考 M. Hall 的《组合论》[32]一书.

(1.3.1)定义. 设 S 是一个含 v 个元素的集合,$\mathscr{B}$ 是以 S 的子集为元素作成的集合(这些子集称为(区)组),使得

(i) 对于每个 $B \in \mathscr{B}$, $|B| = k$,

(ii) 对于每个满足 $|T| = t$ 的 $T \subset S$, 恰有 λ 个组 B 使得 $T \subset B$,

那么,对 $(S, \mathscr{B})$ 称为一个 t-设计(记为 t-(v, k, λ)). S 的元素称为该设计的点. 若 $\lambda = 1$, 设计称为 Steiner 系.

t-设计常常用一个关联矩阵 A 表示, A 有 $|\mathscr{B}|$ 行 $|S|$ 列,并以组的特征函数作为它的行.

(1.3.2)定义. 具有参数 $(v, k; b, r, \lambda)$ 的区组设计是一个满足 $|\mathscr{B}| = b$ 的 2-(v, k, λ). 对于每个点,有 r 个组包含该点. 如果 $b = v$, 那么这个区组设计叫做对称的.

(1.3.3)定义. n 阶射影平面是一个 2-$(n^2+n+1,\ n+1,\ 1)$. 在这种情况下,组叫做该平面的线. n 阶射影平面记作 PG$(2, n)$.

(1.3.4) 定义． 域 $\mathbf{F}_q$ 上的 m 维仿射几何是向量空间 $(\mathbf{F}_q)^m$（我们用符号 $AG(m, q)$ 表示仿射几何）．一个 k 维仿射子空间或 k-平坦是 k 维子空间（看成子群）的一个陪集．若 $k = m - 1$，我们称这个平坦为超平面．由 $(\mathbf{F}_q)^m$ 的线性变换及向量空间的平移生成的群叫做仿射变换群，并记作 $AGL(m, q)$．§ 1.1 中定义的仿射置换群是 $m = 1$ 时的情形．$\mathbf{F}_q$ 上的 m 维射影几何（记号 $PG(m, q)$）由 $AG(m + 1, q)$ 的线性子空间组成．称 1 维子空间为点，2 维为线，等等．

我们举一个例子．考虑 $AG(3, 3)$，它有 27 个点，$\frac{1}{2}(27 - 1) = 13$ 条线过点 $(0, 0, 0)$ 和 13 个平面过点 $(0, 0, 0)$．这 13 条线是 $PG(2, 3)$ 的“点”，而 $AG(3, 3)$ 中的 13 个平面是这个射影几何的“线”．显然，这是一个 2-(13, 4, 1)．当说到 $PG(m, q)$ 中某个点的坐标时，我们总是指在 $AG(m + 1, q)$ 中任意与之对应的非零点的坐标．因此，在 $PG(2, 3)$ 这个例子中，三元组 $(1, 2, 1)$ 和 $(2, 1, 2)$ 代表 $PG(2, 3)$ 中同一个点的坐标．

(1.3.5) 定义． 一个以 $+1$ 和 -1 为元素，满足 $HH^T = nI$ 的 n 阶方阵 H，称为 Hadamard 矩阵．

(1.3.6) 定义． 一个对角线元素为 0，非对角线元素为 $+1$ 或 -1，且使得 $CC^T = (n - 1)I$ 的 n 阶方阵 C，称为 Conference 矩阵．

有几种人们熟知的构造 Hadamard 矩阵的方法，其中之一基于所谓的矩阵之 Kronecker 积，定义如下：

(1.3.7) 定义． 设 A 是以 a_{ij} 为元素的 $m \times m$ 矩阵，B 是一个 $n \times n$ 矩阵，则 Kronecker 积 $A \otimes B$ 是由下式给出的一个 $mn \times mn$ 矩阵

$$A \otimes B := \begin{bmatrix} a_{11}B & a_{12}B \cdots a_{1m}B \\ a_{21}B & a_{22}B \cdots a_{2m}B \\ \vdots & \vdots \quad \cdots \quad \vdots \\ a_{m1}B & a_{m2}B \cdots a_{mm}B \end{bmatrix}.$$

不难证明，Hadamard 矩阵的 Kronecker 积仍然是 Hadamard

矩阵．从 $H_2 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ 出发，我们可以得到序列 $H_2^{\otimes n}$，其中 $H_2^{\otimes 2} = H_2 \otimes H_2$，等等．这些矩阵将出现在本书的若干地方（有时形式不同）．

另一个最著名的构造方法属于 R. E. A. Paley（见 Hall[32]）．设 q 是一个奇素数的方幂，我们定义 $\mathbf{F}_q$ 上函数 χ 为 $\chi(0) := 0$；$\chi(x) = 1$ 若 x 是非零平方元；$\chi(x) = -1$ 其它．注意 χ 限制在 $\mathbf{F}_q$ 的乘法群上是一个特征标．以任何方式排列 $\mathbf{F}_q$ 中元素：a_0，$a_1, a_2, \cdots, a_{q-1}$，其中 $a_0 = 0$．

(1.3.8)定理． q 阶 Paley 矩阵 S 定义为 $S_{ij} := \chi(a_i - a_j)$，它具有性质：

(i) $SJ = JS = 0$，

(ii) $SS^T = qI - J$，

(iii) $S^T = (-1)^{(q-1)/2} S$．

如果我们取这样一个矩阵 S，按如下作 $q+1$ 阶矩阵 C

$$C = \begin{bmatrix} 0 & 1 & 1 \cdots 1 \\ -1 & & \\ -1 & & \\ \vdots & & S \\ -1 & & \end{bmatrix},$$

则 C 是一个 $q+1$ 阶 Conference 矩阵．若 $q \equiv 3 (\mathrm{mod}\ 4)$，则我们可以考虑 $H := I + C$．因为 -1 在 $\mathbf{F}_q$ 中不是平方元，所以 $C^T = -C$，从而我们看到 H 是一个 $q+1$ 阶 Hadamard 矩阵．

(1.3.9)例．存在一个 12 阶 Hadamard 矩阵．它可由在定理 1.3.8 中取 $q = 11$，并如上构造而得．我们称其为 H_{12}．

§ 1.4 概 率 论

设 $\mathbf{x}$ 是一个可以取有限个值 $x_1, x_2, \cdots$ 的随机变量．象通常一样，我们用 p_i 表示 $\mathbf{x}$ 等于 x_i 的概率，即 $p(\mathbf{x} = x_i) = p_i$．$\mathbf{x}$ 的

均值或期望(值)是 $\mu:=\mathscr{E}(\mathbf{x}):=\sum_i p_i x_i$.

若 g 是定义在 $\mathbf{x}$ 的值域上的函数,那么, $\mathscr{E}(g(\mathbf{x}))=\sum_i p_i\cdot g(x_i)$. 我们将利用一些熟知的性质,如

$$\mathscr{E}(a\mathbf{x}+b\mathbf{y})=a\mathscr{E}(\mathbf{x})+b\mathscr{E}(\mathbf{y}).$$

标准差 σ 和方差 σ^2 定义为: $\mu=\mathscr{E}(\mathbf{x})$,

$$\sigma^2:=\sum_i p_i x_i^2-\mu^2=\mathscr{E}(\mathbf{x}-\mu)^2,\ (\sigma>0).$$

我们还需要若干关于 2 维分布的结论. 记 $p_{ij}:=P(\mathbf{x}=x_i\wedge\mathbf{y}=y_j)$, $p_i:=P(\mathbf{x}=x_i)=\sum_j p_{ij}$. 条件概率记为 $P(\mathbf{x}=x_i|\mathbf{y}=y_j)=p_{ij}/p_j$. 我们说 $\mathbf{x}$ 和 $\mathbf{y}$ 是独立的,如果对所有的 i,j 都有 $p_{ij}=p_i p_j$. 在这种情况下,我们有

$$\mathscr{E}(\mathbf{xy})=\sum_{i,j} p_{ij}x_i y_j=\mathscr{E}(\mathbf{x})\mathscr{E}(\mathbf{y}).$$

所有这些事实都可以在概率论的标准教科书中找到(例如 W. Feller [21]),下述结论(将在第二章中用到)也不例外.

(1.4.1)定理 (Chebyshev 不等式). 设 $\mathbf{x}$ 是一个随机变量, 其均值为 μ,方差为 σ^2,则对任何 $k>0$,

$$P(|\mathbf{x}-\mu|\geqslant k\sigma)<k^{-2}.$$

在下一章中起最重要作用的分布是二项分布. 这里 $\mathbf{x}$ 取值为 $0,1,\cdots,n$, $P(\mathbf{x}=i)=\binom{n}{i}p^i q^{n-i}$, 其中 $0\leqslant p\leqslant 1$, $q:=1-p$. 对于这个分布我们有 $\mu=np$, $\sigma^2=np(1-p)$. 估计二项分布系数的一个重要工具是下述定理.

(1.4.2)定理 (Stirling 公式).

$$\begin{aligned}\log n! &= \left(n+\frac{1}{2}\right)\log n-n+\frac{1}{2}\log(2n)+o(1),\quad (n\to\infty)\\ &= n\log n-n+O(\log n),\quad (n\to\infty).\end{aligned}$$

另一个关于二项系数的十分有用的引理是

(1.4.3)引理. 我们有

$$\binom{n}{m} \leqslant \frac{n^n}{m^m(n-m)^{n-m}}.$$

证明.

$$n^n = \{m + (n-m)\}^n \geqslant \binom{n}{m} m^m (n-m)^{n-m}. \qquad \square$$

现在我们引进一个在信息论中十分重要的函数，称为二元熵函数，通常记为 H. 在(5.1.5)中我们还将把它从二元推广到 q 元. 下面的对数以 2 为底.

(1.4.4)定义. 二元熵函数 H 定义为

$$H(0) := 0,$$

$$H(x) := -x\log x - (1-x)\log(1-x),$$

$$(0 < x \leqslant 1/2).$$

(1.4.5)定理. 设 $0 \leqslant \lambda \leqslant \frac{1}{2}$, 则有

(i) $\displaystyle\sum_{0\leqslant i\leqslant \lambda n} \binom{n}{i} \leqslant 2^{nH(\lambda)}$,

(ii) $\displaystyle\lim_{n\to\infty} n^{-1}\log \sum_{0\leqslant i\leqslant \lambda n} \binom{n}{i} = H(\lambda)$.

证明.

(i) $$1 = \{\lambda + (1-\lambda)\}^n \geqslant \sum_{0\leqslant i\leqslant \lambda n} \binom{n}{i} \lambda^i (1-\lambda)^{n-i}$$

$$\geqslant \sum_{0\leqslant i\leqslant \lambda n} \binom{n}{i} (1-\lambda)^n \left(\frac{\lambda}{1-\lambda}\right)^{\lambda n}$$

$$= 2^{-nH(\lambda)} \sum_{0\leqslant i\leqslant \lambda n} \binom{n}{i}.$$

(ii) 记 $m := \lfloor \lambda n \rfloor$, 则 $m = \lambda n + O(1)$, $n \to \infty$. 因此由定理 1.4.2 我们看到

$$n^{-1}\log \sum_{0\leqslant i\leqslant \lambda n} \binom{n}{i} \geqslant n^{-1}\log \binom{n}{m}$$

$$
\begin{aligned}
&= n^{-1}\{n\log n - m\log m - (n-m) \\
&\qquad \cdot \log(n-m) + o(n)\} \\
&= \log n - \lambda\log(\lambda n) - (1-\lambda)\log((1-\lambda)n) + o(1) \\
&= H(\lambda) + o(1),\ n\to\infty.
\end{aligned}
$$

由 (i) 即得结论. □

第二章 Shannon 理论

§2.1 引 言

本书将对纠错编码理论的数学方面作一介绍．这一理论应用于具有下述共同特征的许多情况：来自某个信源的消息通过一个噪声信道送到收方．例如电话交谈、存储设备(如为计算机输送储存信息的磁带元件)、电报等．下面则是一个典型的近期例子．很多读者可能看到过航海者号、旅行者号等人造卫星拍摄的火星、土星以及其它行星的精彩照片．为了把这些照片送到地球上，在照片上要搁置一块精制的带方格铁片，铁片的每个方格的明暗程度用比方说 0—63 个等级标出．这些数用二进制表示，也就是说，每个小方格对应一串长为六的 0 和 1 的数． 0 和 1 作为两个不同的信号传送到地球上(在 Pasadena 的加州理工学院喷气动力实验室)．信号到达地面时十分微弱，因此必须放大．由于热噪声的影响，偶而会发生这种情况：信号发出时为 0，但接收器却译成了 1；或者反之．如果上述提到的 0 和 1 的 6 元组就这样传送，那么接收器的错译会对照片产生很大影响．为了避免这一缺点，在信号中加入了所谓的多余度，也就是说，被传送的序列所包含的内容多于必须的信息．我们在日常用语中已经熟悉多余性的原则了．英语语言中的词只是所有可能的字母(符号)串的一小部分，所以我们能辨认出一个较长的词中出现的一个印刷错误．这是因为这个词显得更接近那个正确的词，而对我们所知道的其它词就不那么接近．这是本书论述的理论的实质．在上述例子中，读者改正印刷错误．一个更合适的噪声信道的编码例子是用于计算机纸带上的系统．为了表示 32 个不同符号，可以用 0 和 1 的 5 元组(即 0 到 31 到二进制表示)．在实际应用中，我们在 5 元组中加进一

个多余比特(二元数字)，使得到的6元组含偶数个1. 使用这种纸带的计算机极少出现错误，但也有可能偶尔出现一个不正确比特. 这时6元组的奇偶性就错了，即含奇数个1. 在这种情况下，机器停止工作(因为它检测到一个错误). 这是一个所谓单一差错检测码的例子.

我们上面提到在照片传送中(例如航海者号1969)，0和1的6元组用更长的0，1串(我们总是称之为字)来代替. 事实上，航海者号所用的字由32个符号组成(见[56]). 此时，读者可能已经知道，人们设计了某种装置，用以把64种可能的信息串(0和1的6元组)改变为64个可能的码字(0和1的32元组). 这种装置叫做编码器. 码字通过编码器传送出来. 我们把随机干扰，即差错看成是加到信息上的某种东西(模2加).

在接收端，一个叫做译码器的装置把32元组译成6元组. 但如果收到的不是允许的64个码字之一，那么译码器先将它译成与其最象的那个码字，然后确定对应的6元组(铁片一个格子的黑色程度). 我们刚刚描述的这个码具有性质：如果32个符号中的差错不超过7个，那么译码器总能作出正确的选择. 当然，我们必须认识到，为了获得这种改正差错的能力而付出的代价，即传送一张照片所需要的时间是没有编码时的5倍多. 图1是上述过程的一个模型.

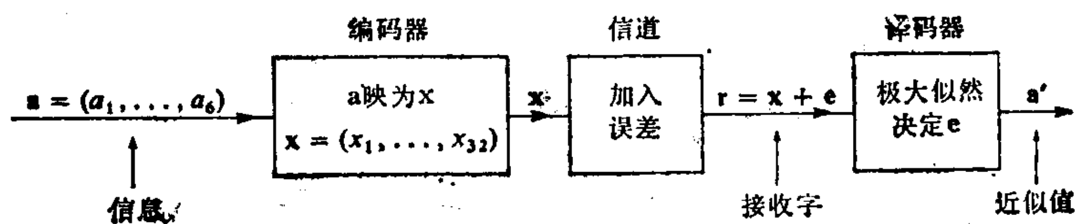


图 1

在本书中，我们的兴趣主要在于构造和分析好码. 在一些情况下，我们也讨论译码的数学问题，但不考虑如何实现. 即使对于同一个码 C，都会有许多不同的方法设计译码器的算计. 一个完全的译码算法把每个可能收到的字都译成某个码字. 在有些情况

下，即我们很不希望出现译码差错时，不完全译码算法反而更可取。这种算法能纠正含少量差错的消息，而对于其它可能接收到的消息将出现译码故障，此时，译码器或者忽略这个消息，或者(可能的话)请求再发. 另一种区分方法是所谓的难以确定和容易确定. 这是有关接收符号的译解的. 对于大多数接收符号，译码器可以毫无疑问地确定它们是 0 还是1，然而有些情形就不是这么回事了，于是我们宁愿记一个？而不去断定这个符号是 0 还是 1. 这类现象常称为删除.

Shannon 理论介绍

为了使读者对编码理论的起源有个较好的认识，我们考虑下面的实验.

我们在一个房间里，有人正以每分钟 l 次的速度掷一枚硬币. 房间用电话线与另一个房间相连. 假定我们可以在这个信道上传送两个不同符号，称之为 0 和 1. 信道是有干扰的，设接收端把传送的 0 译为 1 或把 1 译为 0 的概率均为 p. 这种信道称为二元对称信道(简记为 B. S. C.). 进一步假设信道每分钟能处理 $2l$ 个符号，而且如果掷硬币进行 T 分钟，那么信道可以使用 T 分钟. 出现正面时我们传送一个 0，出现反面则传送一个 1. 在接收端，接收信息不正确的概率为小数 p. 现在，如果没有上面规定的时间限制，我们可以达到任意小的差错概率. 方法如下：设 N 是奇数，则我们传送 N 个 0 (或 1) 而不是一个 0 (或 1). 接收器考虑所收到的 N 元组，把它译成出现次数较多的那个符号. 这个码叫做长为 N 的重复码，它由两个码字即 $\mathbf{0}=(0,0,\cdots,0)$ 和 $\mathbf{1}=(1,1,\cdots,1)$ 组成. 作为例子，我们取 $p=0.001$，则译码器出现一次错译的概率为

$$(2.1.1)\qquad \sum_{0\leqslant k\leqslant N/2}\binom{N}{k}q^kp^{N-k}<(0.07)^N,\ (\text{这里 } q:=1-p),$$

当 $N\to\infty$ 时这个概率趋于 0((2.1.1) 的证明是练习 2.4.1).

由于受时间限制，我们遇到了严重问题！把每个符号发送两

次而不是一次是毫无意义的. C. E. Shannon (见[62])的一个十分著名的定理说,在这里所述的情况下,我们仍然可以在接收端获得任意小的差错概率. 证明将在下节给出, 但是证明的基本思想可从下面得到. 我们按下述方法传送掷两次硬币的结果:

正面,正面⟶ 0 0 0 0,

正面,反面⟶ 0 1 1 1,

反面,正面⟶ 1 0 0 1,

反面,反面⟶ 1 1 1 0.

我们看到前面两个传送符号是实际信息,后两个是多余的. 译码器使用下列完全译码算法: 若收到的 4 元组不是上述之一, 则假定第 4 个符号是正确的, 而前三个符号中有一个差错. 任何收到的 4 元组都可以唯一译解出来. 如果上述假定为真, 则结果是对的. 未经编码,两个结果正确接收的概率为 $q^2 = 0.998$,而用上述方法编码后其概率为 $q^4 + 3q^3p = 0.999$. 左边第二项是收到的字含一个错、且不在第 4 位的概率. 因此,我们有了一个很好的改进, 而且得来容易. 时间的要求也满足了. 我们把上述思想推广到一次传送掷三次硬币的结果. 此时我们要传送的信息是 0 和 1 的 3 元组,譬如 (a_1, a_2, a_3). 不过实际传送的不是 3 元组,而是 6 元组 $(a_1, \cdots, a_6)$,其中 $a_4 := a_2 + a_3$, $a_5 := a_1 + a_3$, $a_6 := a_1 + a_2$(加法模 2). 我们已经构造了一个由八个码字组成的码, 码字长为 6. 如前所述, 我们把干扰看成是加到信息上的某种东西,即收到的字 $\mathbf{b}$ 是 $\mathbf{a} + \mathbf{e}$, 其中 $\mathbf{e} = (e_1, e_2, \cdots, e_6)$ 称为**差错模式**(差错向量). 我们有

$$e_2 + e_3 + e_4 = b_2 + b_3 + b_4 := s_1,$$

$$e_1 + e_3 + e_5 = b_1 + b_3 + b_5 := s_2,$$

$$e_1 + e_2 + e_6 = b_1 + b_2 + b_6 := s_3.$$

因为接收端知道 $\mathbf{b}$, 所以也知道 s_1, s_2, s_3. 给定 s_1, s_2, s_3 后、译码器必须选择最有可能的差错模式 $\mathbf{e}$ 使其满足三个方程. 最有可能的差错模式就是含符号 1 最少的 $\mathbf{e}$. 我们容易看到,若 $(s_1, s_2, s_3) \neq (1, 1, 1)$, 则 $\mathbf{e}$ 的选择是唯一的. 若 $(s_1, s_2, s_3) = (1, 1, 1)$,

则译码器必须选择 $(1, 0, 0, 1, 0, 0)$, $(0, 1, 0, 0, 1, 0)$, $(0, 0, 1, 0, 0, 1)$ 这三种可能之一作为 **e**. 我们看到含一个错的差错模式可以正确译解. 在所有其它差错模式中，有一个含两个错的可以正确译码. 因此经过译码，三个符号 a_1, a_2, a_3 都能正确译解的概率是

$$q^6 + 6q^5p + q^4p^2 = 0.999986.$$

这已经是一个巨大的改进了.

通过这段介绍，读者不难理解编码理论的下列重要概念

(2.1.2)定义. 若码 C 由长为 n 的字组成，则

$$R := n^{-1}\log_2|C|$$

称为这个码的信息率(或简称(码)率).

码率的概念与上面讨论的关于传送信息所需的时间有关. 在纸带的 32 个可能字的例子中，码率是 $\frac{5}{6}$, 航海者 1969 使用了信息率为 $\frac{6}{32}$ 的码，这与我们所说的传送信息所需时间是没有编码时的 5 倍多是一致的. 定义信息率前举的例子中，$R = \frac{1}{2}$.

我们曾提到航海者 1969 使用的码具有性质: 接收端能改正不多于 7 个错误的任何接收到的字. 这之所以可能是因为任何两个不同的码字至少有 16 个位置相异. 因此，含少于 8 个错误的接收到的字与任何其它码字相比，更象所要的那个码字. 这导致下述定义:

(2.1.3)定义. 若 $\mathbf{x}$ 和 $\mathbf{y}$ 是两个 0 和 1 的 n 元组，则我们说它们的 Hamming 距离(通常简称距离)是

$$d(\mathbf{x}, \mathbf{y}) := |\{i \mid 1 \leqslant i \leqslant n,\ x_i \neq y_i\}|.$$

(见(3.1.1).)

我们前面讨论的由长为 6 的八个码字组成的码 C 具有任意两个不同码字之间的距离至少为 3 的性质. 这就是为什么它能纠正一个差错的原因所在. 这个码是单一纠错码.

我们所遵循的译码原则基于两个假设．首先我们假定在通信过程中，所有码字都是等可能的；其次我们利用了下列事实，即若 $n_1 > n_2$，则含 n_1 个错的差错模式比含 n_2 个错的差错模式出现的可能性要小．

这意味着如果收到 $\mathbf{y}$，则我们要找一个码字 $\mathbf{x}$ 使得 $d(\mathbf{x}, \mathbf{y})$ 最小，这一原则叫做**极大似然译码法**．

§ 2.2 Shannon 定理

现在我们将就 § 2.1 所给例子的情形叙述并证明 Shannon 定理．先叙述问题：我们有一个二元对称信道，接收一个符号出现错误的概率为 p（仍记 $q := 1 - p$）．假定我们使用的是一个长为 n，由 M 个码字组成的码 C，并且每个码字的出现是等概率的．设 $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M$ 是码字，我们用极大似然译码法．令 P_i 是传送 x_i 作出不正确决定的概率．在这种情况下，一个接收字的错误译码概率为

(2.2.1) $$P_C := M^{-1} \sum_{i=1}^{M} P_i.$$

现在考虑所有可能的具有给定参数的码 C，定义

(2.2.2) $$P^*(M, n, p) := P_C \text{ 的极小值}.$$

(2.2.3)定理 (Shannon 1948)． 若 $0 < R < 1 + p\log p + q\log q$，且 $M := 2^{\lfloor Rn \rfloor}$，则 $P^*(M_n, n, p) \to 0$，当 $n \to \infty$．

（这里所有对数以 2 为底．）我们指出，在上一节的例子中 $p = 0.001$，即 $1 + p\log p + q\log q$ 很接近 1．在实验中要求码率至少为$\frac{1}{2}$．我们看到对于 $\varepsilon > 0$ 和充分大的 n，存在长为 n 的码 C，其码率接近 1，且使得 $P_C < \varepsilon$（当然 T 太小时码长不能太大）．

在给出定理 2.2.3 的证明之前，我们先处理若干后面要用的技术细节．

出现 w 个错的差错模式的概率是 $p^w q^{n-w}$，也就是说，它只依

赖于 w. 我们注意到传送 $\mathbf{x}$, 收到 $\mathbf{y}$ 的概率(记作 $P(\mathbf{y}|\mathbf{x})$) 等于 $P(\mathbf{x}|\mathbf{y})$.

一个接收字中的差错个数是一个随机变量，其期望值是 np, 方差是 $np(1-p)$. 若 $b:=(np(1-p)/(\varepsilon/2))^{1/2}$,则由 Chebyshev 不等式(定理 1.4.1) 我们有

$$(2.2.4)\qquad P(w > np + b) \leqslant \frac{1}{2}\varepsilon.$$

因为 $p < \frac{1}{2}$,所以当 n 充分大时 $\rho:=\lfloor np + b\rfloor$小于$\frac{1}{2}n$. 设 $B_\rho(\mathbf{x})$ 是满足 $d(\mathbf{x}, \mathbf{y}) \leqslant \rho$ 的字 $\mathbf{y}$ 的集合,那么

$$(2.2.5)\qquad |B_\rho(\mathbf{x})| = \sum_{i\leqslant\rho}\binom{n}{i} \leqslant \frac{1}{2}n\binom{n}{\rho} \leqslant \frac{1}{2}n\cdot\frac{n^n}{\rho^\rho(n-\rho)^{n-\rho}}$$

(见引理 1.4.3). 集合 $B_\rho(\mathbf{x})$ 通常称为以 $\mathbf{x}$ 为中心，以 ρ 为半径的球.

我们要用到下列估计:

$$(2.2.6)\quad \frac{\rho}{n}\log\frac{\rho}{n} = \frac{1}{n}\lfloor np + b\rfloor\log\frac{\lfloor np+b\rfloor}{n} = p\log p + O(n^{-1/2}),$$

$$\left(1-\frac{\rho}{n}\right)\log\left(1-\frac{\rho}{n}\right) = q\log q + O(n^{-1/2}), \quad (n\to\infty).$$

最后,我们引进几个在证明中有作用的函数. 设

$$\mathbf{u}\in\{0, 1\}^n, \quad \mathbf{v}\in\{0, 1\}^n,$$

则

$$(2.2.7)\qquad f(\mathbf{u}, \mathbf{v}):=\begin{cases}0, & 若\ d(\mathbf{u}, \mathbf{v}) > \rho,\\ 1, & 若\ d(\mathbf{u}, \mathbf{v}) \leqslant \rho.\end{cases}$$

若 $\mathbf{x}_i\in C$, $\mathbf{y}\in\{0, 1\}^n$, 则

$$(2.2.8)\qquad g_i(\mathbf{y}):=1 - f(\mathbf{y}, \mathbf{x}_i) + \sum_{j\neq i} f(\mathbf{y}, \mathbf{x}_j).$$

注意: 如果 $\mathbf{x}_i$ 是唯一使 $d(\mathbf{x}_i, \mathbf{y}) \leqslant \rho$ 的码字,那么 $g_i(\mathbf{y}) = 0$, 否则 $g_i(\mathbf{y}) \geqslant 1$.

定理 2.2.3 之证明．在 Shannon 定理的证明中，我们(独立地)随机选取码字 $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M$．我们按下述方法译码．设收到 $\mathbf{y}$，若恰好存在一个码字 $\mathbf{x}_i$ 使得 $d(\mathbf{x}_i, \mathbf{y}) \leqslant \rho$，那么就把 $\mathbf{y}$ 译为 $\mathbf{x}_i$，否则我们声明有一个错(如果必须译，我们总译为 $\mathbf{x}_1$)．

令 P_i 定义如上．我们有

$$\begin{aligned} P_i &\leqslant \sum_{\mathbf{y}\in\{0,1\}^n} P(\mathbf{y}\mid\mathbf{x}_i)g_i(\mathbf{y}) \\ &= \sum_{\mathbf{y}} P(\mathbf{y}\mid\mathbf{x}_i)\{1 - f(\mathbf{y}, \mathbf{x}_i)\} \\ &\quad + \sum_{\mathbf{y}}\sum_{j\neq i} P(\mathbf{y}\mid\mathbf{x}_i)f(\mathbf{y}, \mathbf{x}_j). \end{aligned}$$

这里右边第一项是接收字 $\mathbf{y}$ 不在 $B_\rho(\mathbf{x}_i)$ 中的概率，由(2.2.4)这个概率至多为 $\frac{1}{2}\varepsilon$．

因此我们有

$$P_C \leqslant \frac{1}{2}\varepsilon + M^{-1}\sum_{i=1}^{M}\sum_{\mathbf{y}}\sum_{j\neq i} P(\mathbf{y}\mid\mathbf{x}_i)f(\mathbf{y}, \mathbf{x}_j).$$

证明的要点是下列事实：$P^*(M, n, p)$ 小于所有可能的随机选取的码 C 上的期望值．从而得

$$\begin{aligned} P^*(M, n, p) &\leqslant \frac{1}{2}\varepsilon + M^{-1}\sum_{i=1}^{M}\sum_{\mathbf{y}}\sum_{j\neq i} \mathscr{E}(P(\mathbf{y}\mid\mathbf{x}_i))\mathscr{E}(f(\mathbf{y},\mathbf{x}_j)) \\ &= \frac{1}{2}\varepsilon + M^{-1}\sum_{i=1}^{M}\sum_{\mathbf{y}}\sum_{j\neq i} \mathscr{E}(P(\mathbf{y}\mid\mathbf{x}_i)) \cdot \frac{|B_\rho|}{2^n} \\ &= \frac{1}{2}\varepsilon + (M-1)2^{-n}|B_\rho|. \end{aligned}$$

我们取对数，再应用(2.2.5)和(2.2.6)，最后除以 n，结果为

$$\begin{aligned} n^{-1}\log\left(P^*(M, n, p) - \frac{1}{2}\varepsilon\right) &\leqslant n^{-1}\log M \\ &\quad - (1 + p\log p + q\log q) + O(n^{-\frac{1}{2}}). \end{aligned}$$

用 $M = M_n$ 替换右边，并利用 R 的限制条件，我们得到，对于 $n > n_0$

$$n^{-1}\log\left(P^*(M, n, p)-\frac{1}{2}\varepsilon\right)<-\beta<0,$$

即 $P^*(M, n, p)<\frac{1}{2}\varepsilon+2^{-\beta n}$.

这就证明了定理.

§2.3 评　注

C. E. Shannon 的"通信的数学理论"一文标志了编码理论的开端. 因为定理证明了好码是存在的，人们就很自然地试图去构造这些码. 但是这些码通常只能使用在很小的电子设备中，所以大家又特别感兴趣于那些具有较多结构，而译码算法相对简单的码. 在后面几章中我们会看到，要想获得规律性很强的码而不失去定理 2.2.3 所示性质是多么困难. 我们知道,编码理论应用的一个重要领域是电话通信，所以读者在本书中将会看到的许多名字是贝尔电话实验室(Bell Telephone Laboratories)以前的研究人员的名字. 除 Shannon 外,还有 Berlekamp, Gilbert, Hamming, Lloyd, MacWilliams, Slepian 和 Sloane 等. 因此毫不奇怪，大量编码理论的早期文献可以在贝尔系统技术杂志 (Bell System Technical Journal) 上找到. 作者的大部分编码理论方面的知识就是在对贝尔实验室的多次访问中获得的，在此深表感激. 如果读者对航海者 1969 使用的码的细节有兴趣,可参考文献[56].

查阅一下参考文献,读者可以看出，迄今为止的许多年来,编码理论的最重要的结果都发表在 *IEEE* 信息论学报 (*IEEE Transactions on Information Theory*) 上.

§2.4 问　题

2.4.1. 证明(2.1.1).

2.4.2. 考虑 §2.2 掷硬币实验所述的长为 6 的码. 我们证明了一

个接收字正确译解的概率是 $q^6+6q^5p+q^4p^2$. 现在假定译码后我们只保留每个接收字的前三个符号（即掷硬币实验的信息），试求序列中有一个符号出错的概率(称为符号差错概率,没有编码时为 p).

2.4.3. 构造一个长为 7、含 8 个字的码,使得任意两个不同码字之间的距离至少是 4. 试就差错概率为 p 的 B. S. C. 求出一个接收字正确译解的概率.

2.4.4. 已知一个二元信道正确接收一个传送符号的概率为 $q=0.9$，而出现一个删除(即收到?)的概率为 $p=0.1$. 我们希望在这个信道上使用一个码率为 $\frac{1}{2}$ 的码. 问如果我们重复发送每个符号，正确译码的概率是否增加? 是不是有可能构造一个长为 6、含 8 个字的码,使得出现两个删除没有什么影响? 比较这两个码正确译码的概率. (假定接收端不能用猜符号的方法改掉删除.)

第三章 线 性 码

§3.1 分 组 码

本章我们假定信息是用含有 q 个不同符号的字母表 Q 进行编码的. 一个码称为分组码(或简称组码), 如果编了码的信息能分成 n 个符号一组,且每组能独立地进行译码. 这些组就是码字, n 叫做分组长度或字长(或就叫长). 第二章举的例子都是组码. 在第十一章中我们将简单地讨论一个完全不同的系统, 叫做卷积编码. 在这种系统中,我们把一个无限信息符号序列 $i_0, i_1, i_2, \cdots$ 编码成另一个无限信息符号序列. 例如对于率 $\frac{1}{2}$ 的码,我们可以有 $i_0, i_1, i_2, \cdots \to i_0, i_0', i_1, i_1', \cdots$, 其中 i_n' 是 $i_0, i_1, \cdots, i_n$ 的函数. 对于组码我们把(2.1.3)推广到任意字母表.

(3.1.1)定义. 设 $\mathbf{x} \in Q^n$, $\mathbf{y} \in Q^n$, 则 $\mathbf{x}$ 和 $\mathbf{y}$ 的距离 $d(\mathbf{x}, \mathbf{y})$ 定义为

$$d(\mathbf{x}, \mathbf{y}) := |\{i \mid 1 \leqslant i \leqslant n, x_i \neq y_i\}|.$$

$\mathbf{x}$ 的重量 $w(\mathbf{x})$ 定义为

$$w(\mathbf{x}) := d(\mathbf{x}, \mathbf{0}).$$

(我们总是用 $\mathbf{0}$ 表示 $(0, 0, \cdots, 0)$, 用 $\mathbf{1}$ 表示 $(1, 1, \cdots, 1)$.)

(3.1.1)定义的距离(仍然称为 Hamming 距离) 确实是 Q^n 上的一个度量. 如果我们使用的信道具有性质: 第 i 位置的差错不影响其它位置, 并且出现差错的符号等概率地可以是其余 $q-1$ 个符号中的任何一个, 那么 Hamming 距离是衡量接收信息中含错内容的一个良好方法. 在第十章我们将会看到,在其它情形,一个与此不同的距离函数更为合适.

在下文中,一个码 C 指的是 Q^n 的一个非空真子集. 若 $|C| =$

1，我们就说这个码是平凡的．若 $q=2$，码称为二元码，$q=3$ 则称为三元码，等等．下列概念在本书中起着基本作用（见第二章）．

(3.1.2)定义． 一个非平凡码 C 的极小距离是

$$\min\{d(\mathbf{x},\mathbf{y})\mid\mathbf{x}\in C,\mathbf{y}\in C,\mathbf{x}\neq\mathbf{y}\}.$$

C 的极小重量是

$$\min\{w(\mathbf{x})\mid\mathbf{x}\in C,\mathbf{x}\neq 0\}.$$

我们也推广码率的概念．

(3.1.3)定义． 若 $|Q|=q$，$C\subset Q^n$，则

$$R:=n^{-1}\log_q|C|$$

称为 C 的(信息)率．

有时我们希望知道一个接收字距最近的码字究竟有多远，为此我们引进一个与极小距离相似的概念．

(3.1.4)定义． 若 $C\subset Q^n$，则 C 的覆盖半径 $\rho(C)$ 为

$$\max\{\min\{d(\mathbf{x},\mathbf{c})\mid\mathbf{c}\in C\}\mid\mathbf{x}\in Q^n\}.$$

我们提醒读者，第二章中以 $\mathbf{x}$ 为中心，ρ 为半径的球 $B_\rho(\mathbf{x})$ 定义为集合 $\{\mathbf{y}\in Q^n\mid d(\mathbf{x},\mathbf{y})\leqslant\rho\}$．因此码 C 的极小距离是使得球 $B_\rho(\mathbf{c})$，$\mathbf{c}\in C$ 不交的最大的 ρ．而覆盖半径是使得 Q^n 包含在 $B_\rho(\mathbf{c})$，$\mathbf{c}\in C$ 的并中的最小的 ρ．若两者相等，则称 C 是完全码．完全码亦可定义如下：

(3.1.5)定义． 一个极小距离为 $2e+1$ 的码 $C\subset Q^n$ 称为完全码，如果每个 $\mathbf{x}\in Q^n$ 都恰与一个码字之间的距离 $\leqslant e$．

极小距离为 $2e+1$ 意味着这个码是 e-纠错的．下述结论是显然的．

(3.1.6)球覆盖条件

若 $C\subset Q^n$ 是一个完全 e-纠错码，则

$$|C|\sum_{i=0}^{e}\binom{n}{i}(q-1)^i=q^n.$$

平凡码显然是完全的(虽然对它无极小距离可言)．第二章我们讨论过完全码的一个简单例子，即由 **0** 和 **1** 组成的长为奇数 n

的二元重复码.

§3.2 线 性 码

现在我们回到构造具有某些代数结构的码这个问题上来. 最初的想法是取一个群 Q 作为字母表,取 Q^n 的子群 C 作为码. 这种码叫做群码. 但在这一节(事实上在本书的大部分)中,我们要求 Q 有更多的结构. 在下面, Q 是一个域 $\mathbf{F}_q$,其中 $q = p^r$ (p 素数). 于是 Q^n 是 n 维向量空间,我们把它记为 $\mathscr{R}^{(n)}$ 或 $\mathscr{R}$. 在后面的几章中. 我们有时要用到 Q^n 同构于 $\mathbf{F}_{q^n}$ 的加群这个事实(见 §1.1).

(3.2.1)定义. 一个线性码 C 是 $\mathscr{R}^{(n)}$ 的一个线性子空间. 若 C 的维数是 k, 则说 C 是一个 $[n, k]$ 码.

今后我们将用 $[n, k, d]$ 码表示极小距离为 d, 长为 n 的 k 维线性码. 用 (n, M, d) 码表示任何极小距离为 d, 长为 n 且含 M 个码字的码.

(3.2.2)定义. 线性码 C 的生成矩阵 G 是一个 $k \times n$ 矩阵, 其行向量是 C 的一组基.

如果 G 是 C 的生成矩阵,那么 $C = \{\mathbf{a}G \mid \mathbf{a} \in Q^k\}$. 我们说 G 是标准型的(经常称为约简阶梯型),如果 $G = (I_k, P)$,其中 I_k 是 $k \times k$ 单位矩阵. § 2.1 例子中的 $(6, 8, 3)$ 码是一个线性码,其生成矩阵 $G = (I, J - I)$. 若 G 是标准型,那么一个码字的前 k 个符号称为信息符号. 它们都是可以随意选取的,但一经选定,其余符号(称为奇偶校验符号)便随之而确定. 引言中提到的纸带上使用的码就有一个奇偶校验比特(奇偶校验这一名称由此而得), 其生成矩阵为 $G = (I_5, \mathbf{1}^T)$.

单就纠错能力而言,两个码 C_1 和 C_2 是一样好的, 如果 C_2 可由一个固定的符号位置的置换作用在 C_1 的所有码字上而得到. 我们称这种码是等价的. 有时等价的定义也可以推广到允许 Q 的符号的一个置换(对每个位置). 由线性代数熟知,每个线性码等价于一个生成矩阵为标准型的码.

一般地，一个码称为在 k 个位置上系统的(在这些位置上的符号叫做信息符号)，如果 $|C|=q^k$，且对于这 k 个位置上的每种可能选取都恰有一个码字．所以我们由上看到，一个 $[n, k]$ 码至少在某 k 个位置上是系统的．由于我们可以把信息符号和多余符号分开，所以这些码也叫做可分码．由(3.1.3)，$[n, k]$ 码的信息率是 k/n，这与 n 个符号中有 k 个带有信息的事实是吻合的．

读者可能已经知道，若 C 的极小距离 $d=2e+1$，则它能纠正接收字中直到 e 个的错．若 $d=2e$，则重量为 e 的差错模式总可以检查出来．在一般情况下，如果 C 有 M 个字，那么需要验算 $\binom{M}{2}$ 对码字才能找到 d，但对于线性码，这项工作要容易得多．

(3.2.3)定理． 线性码 C 的极小距离等于极小重量．

证明．$d(\mathbf{x}, \mathbf{y})=d(\mathbf{x}-\mathbf{y}, \mathbf{0})=w(\mathbf{x}-\mathbf{y})$，且若 $\mathbf{x}\in C$，$\mathbf{y}\in C$，则 $\mathbf{x}-\mathbf{y}\in C$． □

(3.2.4)定义． 设 C 是 $[n, k]$ 码，我们定义对偶码 $C^\perp$ 为

$$C^\perp:=\{\mathbf{y}\in \mathscr{R}^{(n)} \mid \forall \mathbf{x}\in C[\langle \mathbf{x}, \mathbf{y}\rangle=0]\}.$$

对偶码显然是线性码，即 $[n, n-k]$ 码．读者应注意，不要以为 $C^\perp$ 就是 $\mathbf{R}$ 上向量空间意义下的正交补．在有限域 Q 的情形，子空间 C 和 $C^\perp$ 可以有大于 $\{\mathbf{0}\}$ 的交．事实上它们甚至可以相等．当 $C=C^\perp$ 时，我们称 C 是自对偶码．

若 $G=(I_k, P)$ 是码 C 的标准型生成矩阵，那么 $H=(-P^{\mathrm{T}}, I_{n-k})$ 是 $C^\perp$ 的生成矩阵，这是因为 H 有合适的大小和秩，并且 $GH^{\mathrm{T}}=0$ 意味着每个码字 $\mathbf{a}G$ 与 H 的每行之内积为 0．换言之，我们有

$$\mathbf{x}\in C \Longleftrightarrow \mathbf{x}H^{\mathrm{T}}=0. \tag{3.2.5}$$

由(3.2.5)，每个码字都必须满足 $n-k$ 个线性方程．

若 $\mathbf{y}\in C^\perp$，则方程 $\langle \mathbf{x}, \mathbf{y}\rangle$ (它对于每个 $\mathbf{x}\in C$ 都成立)称为奇偶校验(方程)，H 叫做 C 的奇偶校验矩阵．在 § 2.1 的 $[6, 3]$ 码中，方程 $a_4=a_2+a_3$ 是奇偶校验之一．

(3.2.6)定义． 设 C 是以 H 为奇偶校验矩阵的线性码，那么对于任

意 $\mathbf{x}\in\mathscr{R}^{(n)}$，我们称 $\mathbf{x}H^{\mathrm{T}}$ 是 $\mathbf{x}$ 的校验子.

从(3.2.5)我们看到，码字由校验子 $\mathbf{0}$ 所刻划．在译解接收向量 $\mathbf{x}$ 时，校验子是一个重要的工具．这个思想还是在§2.1中用 $[6,3]$ 码时引入的．因为 C 是 $\mathscr{R}^{(n)}$ 的子群，我们可以把 $\mathscr{R}^{(n)}$ 划分为 C 的陪集．两个向量 $\mathbf{x}$ 和 $\mathbf{y}$ 在同一个陪集中当且仅当它们有相同的校验子 $(\mathbf{x}H^{\mathrm{T}}=\mathbf{y}H^{\mathrm{T}}\Longleftrightarrow\mathbf{x}-\mathbf{y}\in C)$．因此，若接收了一个差错模式为 $\mathbf{e}$ 的向量 $\mathbf{x}$，则 $\mathbf{x}$ 和 $\mathbf{e}$ 有相同的校验子．由此即得，对于用极大似然译码法译 $\mathbf{x}$，我们必须在包含 $\mathbf{x}$ 的陪集中选择一个重量最小的向量 $\mathbf{e}$，然后把 $\mathbf{x}$ 译成 $\mathbf{x}-\mathbf{e}$．向量 $\mathbf{e}$ 称为陪集头．具体做法如§2.1中[6,3]码一例所示．在8个陪集中有7个有唯一的陪集头，只有当校验子 $(s_1,s_2,s_3)=(1,1,1)$ 时，我们才从3个可能的陪集头中任选一个.

至此，我们看到引进代数结构的第一个巨大的优越性：$\mathbf{F}_q$ 上的 $[n,k]$ 码有 q^k 个码字和 q^n 个可能收到的消息．假定码有较高的信息率，那么接收者需要知道对应于所有可能的校验子的 q^{n-k} 个陪集头．而现在 q^{n-k} 比 q^n 要小得多．要是码没有结构，那么对于每个可能收到的字 $\mathbf{x}$，我们都得列出最有可能发送的字.

显然，若 C 的极小距离为 $d=2e+1$，则每个重量 $\leqslant e$ 的差错模式都是某个陪集的唯一陪集头．这是因为两个重量 $\leqslant e$ 的向量的距离 $\leqslant 2e$，因而它们在不同的陪集中．若 C 是完全的，则没有其它陪集头．若 C 的极小距离是 $2e+1$，而所有陪集头的重量 $\leqslant e+1$，那么 C 称为拟完全码．§2.1的 $[6,3]$ 码是一个例子.

我们另举一个译码过程十分简单的例子（见[3]）．设 C 是以 $G=(I_k,P)$ 为生成矩阵的二元自对偶 $[2k,k]$ 码．如果 C 能纠正3个错，而且收到的字中出现3个以上错的概率很小，那么这个译码算法是可行的．奇偶校验矩阵 $H=(P^{\mathrm{T}},I_k)$，但由于 C 是自对偶的，所以 G 也是奇偶校验矩阵．令 $\mathbf{y}=\mathbf{c}+\mathbf{e}$ 是一个接收字，我们把 $\mathbf{e}$ 写成 $(\mathbf{e}_1;\mathbf{e}_2)$，其中 $\mathbf{e}_1$ 对应前 k 个位置，$\mathbf{e}_2$ 对应后 k 个位置．我们计算两个校验子：

$$\mathbf{s}^{(1)}:=\mathbf{y}H^{\mathrm{T}}=\mathbf{e}_1P+\mathbf{e}_2,$$

$$\mathbf{s}^{(2)} := \mathbf{y} G^{\top} = \mathbf{e}_1 + \mathbf{e}_2 P^{\top}.$$

如果 $t \leqslant 3$ 个差错都出现在 y 的前一半或后一半，即 $\mathbf{e}_1 = \mathbf{0}$ 或 $\mathbf{e}_2 = \mathbf{0}$，那么其中一个校验子的重量 $\leqslant 3$，所以我们立即可得 $\mathbf{e}$. 如果不是这样，那么 $t \leqslant 3$ 的假设意味着 $\mathbf{e}_1$ 或 $\mathbf{e}_2$ 的重量为 1. 考虑改变 $\mathbf{y}$ 第 i 个分量得到的 $2k$ 个向量 $\mathbf{y}^{(i)}$ $(1 \leqslant i \leqslant 2k)$. 对于其中每个向量，我们分别计算 $\mathbf{s}_1$（对 $i \leqslant k$）和 $\mathbf{s}_2$（对 $i > k$）. 若能找到一个校验子的重量 $\leqslant 2$，则我们就能纠正其余差错. 若找到重量为 3 校验子，则当 C 的距离为 8 时我们能检查 4 个错，而当 C 的距离 $\geqslant 10$ 时，我们能纠正含 4 个错的这种模式.

按照某种自然的规则，在一个码 C 的每个码字上附加一个符号常常表明是有用的. 最常用的方法是由下列定义给出的.

(3.2.7)定义. 设 C 是字母表 $\mathbf{F}_q$ 上的一个长为 n 的码，则我们定义扩充码 $\bar{C}$ 为

$$\bar{C} := \left\{ (c_1, c_2, \cdots, c_n, c_{n+1}) \mid (c_1, \cdots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0 \right\}.$$

如果 C 是以 G 为生成矩阵、以 H 为奇偶校验矩阵的线性码，那么 $\bar{C}$ 有生成矩阵 $\bar{G}$ 和奇偶校验矩阵 $\bar{H}$，其中 $\bar{G}$ 由 G 加上一列得到，满足 $\bar{G}$ 每行之和为 0；$\bar{H}$ 为

$$\bar{H} := \begin{bmatrix} 1 & 1 & 1 \cdots & 1 \\ & & & 0 \\ & H & & 0 \\ & & & \vdots \\ & & & 0 \end{bmatrix}.$$

若 C 是极小距离为奇数 d 的二元码，则因为 $\bar{C}$ 的所有重量和距离都是偶数，所以 $\bar{C}$ 有极小距离 $d+1$.

§ 3.3 Hamming 码

设 G 是 $\mathbf{F}_q$ 上 $[n, k]$ 码 C 的生成矩阵，其阶为 $k \times n$. 若 G

的任意两列线性独立，即这些列表示 PG$(k-1, q)$ 的不同点，则 C 称为**射影码**. 对偶码 $C^\perp$ 以 G 为奇偶校验矩阵. 设 $\mathbf{c} \in C^\perp$ 且 $\mathbf{e}$ 是重量为 1 的差错向量，那么校验子 $(\mathbf{c}+\mathbf{e})G^T$ 是 G 的某列的倍数，因为这唯一确定了 G 的列，所以我们由此即知，$C^\perp$ 至少可以纠正一个差错. 现在我们来看 n 为极大的情形 (k 给定).

(3.3.1) 定义. 设 $n := (q^k-1)/(q-1)$. $\mathbf{F}_q$ 上的 $[n, n-k]$ Hamming **码**是这样一个码，它的奇偶校验矩阵的列（在 $\mathbf{F}_q$ 上）是两两线性无关的，即这些列是两两线性无关向量的极大集合.

在这里我们显然没有区别等价码. Hamming 码的极小距离显然是 3.

(3.3.2) 定理. Hamming **码是完全码**.

证明. 设 C 是 $\mathbf{F}_q$ 上的 $[n, n-k]$ Hamming 码，其中 $n=(q^k-1)/(q-1)$. 若 $\mathbf{x} \in C$，则

$$|B_1(\mathbf{x})| = 1 + n(q-1) = q^k.$$

所以 q^{n-k} 个以 C 中码字为中心、以 1 为半径的互不相交的球包含 $|C|q^k = q^n$ 个字，也就是说，包含了所有可能的字. 因此 C 是完全的(见(3.1.5)和(3.1.6)). □

(3.3.3)例. [7, 4] Hamming 码的奇偶校验矩阵为

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

若考虑 H 中某两列及它们之和(例如 H 的前三列)，则 C 中有一个重量为 3 的字，其 1 所在的位置对应于这些列所在的位置(例如(1 1 1 0 0 0 0)). 因此 C 有 7 个重量为 3 的码字，把它们排成一个矩阵的行，构成 PG(2, 2). C 中重量为偶数的字是问题 2.4.3 的解答. 观察 H 我们看到，扩充码 $\bar{C}$ 是自对偶的.

§ 3.4 大数逻辑译码

这一节我们简要描述一种可用于许多线性码的译码方法，其

推广将在后几章中给出．这一方法简单，而且在有些情形，它能纠正的差错个数比我们所期望的还要多．

(3.4.1)定义． 一组奇偶校验方程 $\langle \mathbf{x}, \mathbf{y}^{(\nu)} \rangle = 0 (1 \leqslant \nu \leqslant r)$ 叫做**关于位置** i **是正交的**（对于码 C；$\mathbf{y}^{(\nu)} \in C^{\perp}$）如果

(i) $y_i^{(\nu)} = 1 \ (1 \leqslant \nu \leqslant r)$，

(ii) 若 $j \neq i$，则至多对于一个 ν，有 $y_j^{(\nu)} \neq 0$．

现在设 $\mathbf{x}$ 是一个含 $t \leqslant \frac{1}{2} r$ 个错的接收字，则

$$\langle \mathbf{x}, \mathbf{y}^{(\nu)} \rangle \neq 0，\text{对于} \begin{cases} \leqslant t \text{ 个 } \nu，\text{若 } x_i \text{ 正确}, \\ \geqslant r-(t-1) \text{个 } \nu，\text{若 } x_i \text{ 不正确}. \end{cases}$$

因为 $r-(t-1) > t$，所以我们依据 $\langle \mathbf{x}, \mathbf{y}^{(\nu)} \rangle$ 的值（即 0 或非 0）的多数决定 x_i 正确与否．在二元码的情形，我们由此即可纠正差错．如果对于每个 i 都有这样一个正交校验集合，那么我们可以一个位置一个位置地纠正其中的差错．

作为例子，我们考虑[7,4]Hamming 码的对偶码（见(3.3.3)）．奇偶校验方程

$$x_1 + x_2 + x_3 = 0,$$
$$x_1 + x_4 + x_5 = 0,$$
$$x_1 + x_6 + x_7 = 0,$$

关于位置 1 是正交的．设 $\mathbf{x}$ 含 1 个差错，则当 x_1 不正确时，三个方程为 1，1，1；当 x_1 正确时，三个方程中有两个是 0，一个是 1．如果有两个结果为 1，那么出现的差错多于 1 个（该码可以检查 2 个差错）．

§3.5 重量计数子

线性码的极小距离告诉我们，一个接收字可以含多少个差错但我们仍能正确译码．对码的距离作更详细的了解常常是很有必要的．为此，我们引入所谓码的**重量计数子**的概念．

(3.5.1)定义． 设 C 是长为 n 的线性码，A_i 是重量为 i 的码字的个

数，则

$$A(z):=\sum_{i=0}^{n} A_i z^i$$

称为 C 的重量计数子，序列 $(A_i)_{i=0}^{n}$ 称为 C 的重量分布.

作为例子，我们计算长为 n 的二元 Hamming 码的重量计数子. 考虑这个码的奇偶校验矩阵的 $i-1$ 个列，共有 3 种可能:

(i) 这个列之和为 $\mathbf{0}$;

(ii) 这些列之和是其中某一列;

(iii) 这些列之和是余下的列中某一列.

选取 $i-1$ 个列共有 $\binom{n}{i-1}$ 种方法，其中情况 (i) 出现 A_{i-1} 次，情况 (ii) 出现 $(n-(i-2))A_{i-2}$ 次，情况 (iii) 出现 iA_i 次. 所以

$$iA_i=\binom{n}{i-1}-A_{i-1}-(n-i+2)A_{i-2},$$

此式在 $i>n+1$ 时显然成立. 两边同乘 z^{i-1}，并对 i 求和，我们发现

$$A'(z)=(1+z)^n-A(z)-nzA(z)+z^2A'(z).$$

因为 $A(0)=1$，这个微分方程有唯一解:

(3.5.2) $$A(z)=\frac{1}{n+1}(1+z)^n+\frac{n}{n+1}(1+z)^{(n-1)/2}(1-z)^{(n+1)/2}.$$

编码理论中一个最基本的结论是属于 F. J. MacWilliams (1963) 的，它给出了一个线性码的重量计数子与其对偶码的重量计数子之间的关系.

(3.5.3)定理. 设 C 是 $\mathbb{F}_q$ 上一个 $[n,k]$ 码，重量计数子为 $A(z)$. 又设 $B(z)$ 是 $C^\perp$ 的重量计数子. 那么

$$B(z)=q^{-k}(1+(q-1)z)^nA\left(\frac{1-z}{1+(q-1)z}\right),$$

证明. 设 χ 是 $(\mathbf{F}_q, +)$ 的任意一个非平凡特征标. 如前,令 $\mathscr{R} = \mathbf{F}_q^n$. 我们定义

$$g(\mathbf{u}) := \sum_{\mathbf{v}\in\mathscr{R}} \chi(\langle \mathbf{u}, \mathbf{v}\rangle) z^{w(\mathbf{v})}$$

则

$$\sum_{\mathbf{u}\in C} g(\mathbf{u}) := \sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in\mathscr{R}} \chi(\langle \mathbf{u}, \mathbf{v}\rangle) z^{w(\mathbf{v})}$$

$$= \sum_{\mathbf{v}\in\mathscr{R}} z^{w(\mathbf{v})} \sum_{\mathbf{u}\in C} \chi(\langle \mathbf{u}, \mathbf{v}\rangle).$$

若 $\mathbf{v}\in C^{\perp}$, 则内和是 $|C|$,若 $\mathbf{v}\notin C^{\perp}$, 则内和 $\langle \mathbf{u}, \mathbf{v}\rangle$ 取到 $\mathbf{F}_q$ 中每个值的次数相同,即内和为 0. 所以

$$\sum_{\mathbf{u}\in C} g(\mathbf{u}) = |C|\cdot B(z). \tag{3.5.4}$$

把重量函数推广到 $\mathbf{F}_q$ 上: 若 $v = 0$, 则记 $w(v) = 0$, 否则记 $w(v) = 1$. 那么令 $\mathbf{u} = (u_1, u_2, \cdots, u_n)$, $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ 后, 我们由 $g(\mathbf{u})$ 的定义得

$$g(\mathbf{u}) = \sum_{(v_1, v_2, \cdots, v_n)\in\mathscr{R}} z^{w(v_1)+\cdots+w(v_n)}\chi(u_1v_1 + \cdots + u_nv_n)$$

$$= \sum_{(v_1, v_2, \cdots, v_n)\in\mathscr{R}} z^{w(v_1)}\chi(u_1v_1) z^{w(v_2)}\chi(u_2v_2)\cdots z^{w(v_n)}\chi(u_nv_n)$$

$$= \prod_{i=1}^{n} \sum_{v\in\mathbf{F}_q} z^{w(v)}\chi(u_iv_i).$$

在最后的表达式中,内和当 $u_i = 0$ 时等于$1 + (q-1)z$,当 $u_i \neq 0$ 时等于

$$1 + z\sum_{\alpha\in\mathbf{F}_q\setminus\{0\}} \chi(\alpha) = 1 - z.$$

因此

$$g(\mathbf{u}) = (1-z)^{w(\mathbf{u})}(1+(q-1)z)^{n-w(\mathbf{u})}. \tag{3.5.5}$$

由于 $|C| = q^k$, 把(3.5.5)代入(3.5.4)即得定理. □

推广见 § 7.2.

§ 3.6 评　注

D. E. Slepian 和 R. W. Hamming 在二十世纪五十年代写的论文对于线性码这一研究课题产生了巨大影响. 有兴趣了解更多关于大数逻辑译码内容的读者可查看 J. L. Massey 的书 [47]. MacWilliams 定理有几个甚至是到非线性码上的推广，详尽的讨论可在[46]的第五章中找到. (3.5.2)的一个应用请看[42]的第二章.

§ 3.7 问　题

3.7.1. 设 C 是一个极小距离为 7，长为 n 的二元完全码. 证明 $n = 7$ 或 $n = 23$.

3.7.2. 设 C 是 $\mathbf{F}_q$ 上的 $[n, k]$ 码，且在任何 k 个位置的集合上都是系统的. 证明 C 的极小距离 $d = n - k + 1$.

3.7.3. 设 C 是一个满足 $C \subset C^{\perp}$ 的二元 $[2k+1, k]$ 码,试描述 $C^{\perp} \backslash C$.

3.7.4. 设 $\mathscr{R} = \mathbf{F}_2^6$，$\mathbf{x} \in \mathscr{R}$. 试求 $|B_1(\mathbf{x})|$. 是否有可能找到一个集合 $C \subset \mathscr{R}$ 满足 $|C| = 9$ 且对任何 $\mathbf{x} \in C$，$\mathbf{y} \in C$，$\mathbf{x} \neq \mathbf{y}$，距离 $d(\mathbf{x}, \mathbf{y})$ 至少是 3?

3.7.5. 设 C 是 $\mathbf{F}_q$ 上以 G 为生成矩阵的 $[n, k]$ 码，若 G 没有全 0 列,则 C 中码字的重量之和为 $n(q-1)q^{k-1}$. 试证明之.

3.7.6. 设 C 是一个二元 $[n, k]$ 码. 若 C 有重量为奇数的码字,则 C 中重量为偶数的字组成一个 $[n, k-1]$ 码. 试证明之.

3.7.7. 设 C 是一个二元码,生成矩阵为

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

试译解下列接收字：

(a) (1 1 0 1 0 1 1)；

(b) (0 1 1 0 1 1 1)；

(c) (0 1 1 1 0 0 0).

3.7.8. 设 p 是一个素数. $\mathbf{F}_p$ 上是否有[8, 4]自对偶码？

3.7.9. 对于 $q = 2$，令 R_k 表示(3.3.1)中定义的 Hamming 码的码率. 试求 $\lim_{k\to\infty} R_k$.

3.7.10. 设 C 是一个二元码，重量计数子为 $A(z)$，试问 $\bar{C}$ 的重量计数子是什么？长度为 2^k 的扩充二元 Hamming 码的对偶码的重量计数子是什么？

3.7.11. 设 C 是一个二元 $[n, k]$ 码，$A(z)$ 是它的重量计数子. 假定我们在一个差错概率为 p 的二元对称信道上使用 C. 我们的目的仅仅是检测错误. 试问接收一个含错字但不能把错误检测出来的概率是多少？

3.7.12. $\mathbf{F}_2$ 上 $n_1 \times n_2$ 的矩阵显然构成一个 n_1n_2 维向量空间 $\mathscr{R}$. 设 C_i 是极小距离为 d_i 的二元 $[n_i, k_i]$ 码 $(i = 1, 2)$. 又设 C 是 $\mathscr{R}$ 的一个子集，它由这样的矩阵组成：它的行是 C_1 中的码字，列是 C_2 中的码字. 证明 C 是一个极小距离为 d_1d_2 的 $[n_1n_2, d_1d_2]$ 码. 这个码称为 C_1 和 C_2 的**直积**.

3.7.13. 设 C 是一个二元[10, 5]码，生成矩阵为

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

证明 C 在下列意义下是**唯一可译码**的：对于每个接收字 $\mathbf{x}$，存在唯一的码字 $\mathbf{c}$ 使得 $d(\mathbf{x}, \mathbf{c})$ 是极小的.

3.7.14. 我们定义距离为 d 的**字典序最小二元码**如下：字长先不固定. 从 $\mathbf{c}_0 = \mathbf{0}$ 和重量为 d 的字 $\mathbf{c}_1 = (1, 1, \cdots, 1, 0, \cdots, 0)$ 出发，若 $\mathbf{c}_0\mathbf{c}_1, \cdots, \mathbf{c}_{l-1}$ 已经选好，则选取 $\mathbf{c}_l$ 为

按字典序（1 尽可能靠近左边）第一个出现的使得 $d(\mathbf{c}_i, \mathbf{c}_l) \geqslant d\ (0 \leqslant i \leqslant l-1)$ 的字. l 步后，定义码的长度为出现分量 1 的那部分的长度.

(i) 证明选取 2^k 个向量后，字典序最小码是线性码.

(ii) 对于 $d=3$，Hamming 码出现在字典序最小码中，试证明之.

第四章　一些好码

§ 4.1　Hadamard 码及其推广

设 H_n 是一个 n 阶 Hadamard 矩阵（参见(1.3.5)），我们用 0 代替 H_n 和 $-H_n$ 中的元素 -1，这样我们得到 $2n$ 个行，它们都是 $\mathbb{F}_2^n$ 中的元素．由于 Hadamard 矩阵的任意两行的元素在一半分位上相异，我们就构造了一个 $\left(n, 2n, \frac{1}{2}n\right)$ 码．对于 $n=8$，这是一个扩充 Hamming 码．对于 $n=32$，它是我们曾在 § 2.1 中提到过的航海者号在 1969 年所使用的码．一般地，这些码都叫做 Hadamard 码．

从 n 阶 Paley 矩阵 S（见(1.3.8)）出发，我们可以类似地构造一个码 C，它含有码字 $\mathbf{0}$, $\mathbf{1}$ 以及矩阵 $\frac{1}{2}(S+I+J)$ 和 $\frac{1}{2}(-S+I+J)$ 的全部行向量．由定理 1.3.8，C 是一个 $\left(n, 2(n+1), \frac{1}{2}(n-1)\right)$ 码．当 $n=9$ 时，C 由下面矩阵的行向量组成

$$
\begin{bmatrix}
000 & 000 & 000 \\
J & P^2 & P \\
P & J & P^2 \\
P^2 & P & J \\
I & J-P^2 & J-P \\
J-P & I & J-P^2 \\
J-P^2 & J-P & I \\
111 & 111 & 111
\end{bmatrix}, \tag{4.1.1}
$$

其中 I 和 J 都是 3×3 矩阵，并且

$$P = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

§ 4.2 二元 Golay 码

考虑一个[7, 4] Hamming 码 H，它以

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

为奇偶校验阵．容易验证，H由 $\mathbf{0}$，(1101000)的七个循环移位(即 PG(2, 2)) 以及这八个码字的补所组成．设 H^* 是将H中的符号逆序所得到的码，则可知 $\overline{H}$ 和 $\overline{H}^*$ 都是[8, 4]码，且有性质：$\overline{H} \cap \overline{H}^* = \{\mathbf{0}, \mathbf{1}\}$．$\overline{H}$ 和 $\overline{H}^*$ 的极小距离都为 4．我们在前面已经看到，这两个码都是自对偶的．

我们如下构造一个字长为 24 的码 $\overline{C}$：

$$\overline{C} := \{(\mathbf{a} + \mathbf{x}, \mathbf{b} + \mathbf{x}, \mathbf{a} + \mathbf{b} + \mathbf{x}) \mid \mathbf{a} \in \overline{H}, \mathbf{b} \in \overline{H}, \mathbf{x} \in \overline{H}^*\}.$$

让 $\mathbf{a}$ 和 $\mathbf{b}$ 跑遍 $\overline{H}$ 的一组基，$\mathbf{x}$ 跑遍 $\overline{H}^*$ 的一组基，则码字$(\mathbf{a},\mathbf{0},\mathbf{a})$，$(\mathbf{0}, \mathbf{b}, \mathbf{b})$，$(\mathbf{x}, \mathbf{x}, \mathbf{x})$ 之全体就是 $\overline{C}$ 的一组基，即 $\overline{C}$ 是一个 [24, 12]码．$\overline{C}$ 的任意两个基向量(不必相异) 正交．因此 $\overline{C}$ 是自对偶码．又因为所有基向量的重量都能被 4 整除，所以 $\overline{C}$ 的每个码字的重量也能被 4 整除．假设某个非零码字 $\mathbf{c} \in \overline{C}$ 的重量 $w(\mathbf{c}) < 8$．

因为 $\mathbf{a} + \mathbf{x}$，$\mathbf{b} + \mathbf{x}$ 和 $\mathbf{a} + \mathbf{b} + \mathbf{x}$ 显然为偶重量，所以其中之一为 $\mathbf{0}$，因而可得 $\mathbf{x} = \mathbf{0}$ 或 $\mathbf{1}$，不失一般性，可设 $\mathbf{x} = \mathbf{0}$．向量 $\mathbf{a}$，$\mathbf{b}$ 和 $\mathbf{a} + \mathbf{b}$ 的重量为 0，4 或 8．因此只能有 $\mathbf{c} = \mathbf{0}$ 于是 $\overline{C}$ 的极小距离为 8．对 $\overline{C}$ 的每个码字，我们去掉其最后一个分位，则可得到一个极小距离是 7 的[23, 12]码 C，这个码叫做**二元 Golay 码**．它的另一种构造见 § 6.9．

S. L. Snover (1973; 参看 [19], [46])已经证明：任一 $(23, 2^{12}, 7)$ 码都与 C 等价. 对任意 $\mathbf{c} \in C$, 我们有 $|B_3(\mathbf{c})| = \sum_{i=0}^{3}\binom{23}{i} = 2^{11}$, 因此 C 是一个完全码!

由上述构造,我们发现 $\mathbf{1} \in \bar{C}$.因此 $\bar{C}$ 的重量计数子是 $A(z) = 1 + Az^8 + Bz^{12} + Az^{16} + z^{24}$, 其中, $2 + 2A + B = 2^{12}$. 计算 $B(z) = A(z)$ 中 z^2 的系数, 再利用定理 3.5.3, 我们得到 $A = 759$. $\bar{C}$ 中两个重量为 8 的互异码字间的距离不小于 8, 即它们至多在 4 个分位上相重. 由此推出: 给定 5 个分位, 至多有一个重量为 8 的码字在这 5 个分位上都是 1. 重量为 8 的码字覆盖了

$$759 \cdot \binom{8}{5} = \binom{24}{5}$$

个 5-元组,即全部 5-元组! 这就证明了下面的

(4.2.1)定理. *扩充二元 Golay 码中重量为 8 的码字全体构成一个 5 − (24, 8, 1) 设计.*

下面的关于 $\bar{C}$ 的译码算法, 基于定理 4.2.1, 它是 § 3.4 的推广. 设 $\mathbf{y}_i (1 \leqslant i \leqslant 253)$ 是 $\bar{C}$ 中在一个给定分位,譬如第一个分位上为 1 的 253 个码字. 考虑奇偶校验子 $\langle \mathbf{x}, \mathbf{y}_i \rangle (1 \leqslant i \leqslant 253)$, 这里用到 $\bar{C}$ 是自对偶码的事实. 假设 $\mathbf{x}$ 是一个接收到的码字, 含有 $t \leqslant 4$ 个错. 由定理 4.2.1, 奇偶校验为 1 的个数由下表给出:

	x_1 正确	x_1 不正确
$t = 1$	77	253
2	112	176
3	125	141
4	128	128

因此,当 $t \leqslant 3$ 时我们能纠正符号 x_1. 上表的最后一行表明, $\bar{C}$ 可以检测 4 个差错却不能纠正 4 个差错.

我们注意到 § 3.2 所述的关于自对偶码的译码程序, 在运用到

扩充二元 Golay 码时至多计算 $26 \times 12 = 312$ 个奇偶校验子就能求出差错向量的全部分量(假定 $t \leqslant 3$)。

§ 4.3 三元 Golay 码

设 S_5 是(1.3.8)中定义的 5 阶 Paley 阵,即

$$S_5 = \begin{bmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{bmatrix}.$$

考虑以

$$G = \left[\begin{array}{c|c} I_6 & \begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \end{array} \\ & \boxed{\quad S_5 \quad} \end{array}\right]$$

为生成矩阵的三元码 C,它是一个[11, 6]码. 由(1.3.8)可知 $\bar{C}$ 是自对偶的,因此 $\bar{C}$ 中任意码字的重量可被 3 整除. $\bar{C}$ 的生成矩阵 $\bar{G}$ 可由 G 加上列 $(0, -1, -1, -1, -1, -1)^T$ 得到. $\bar{G}$ 的每个行的重量为 6, $\bar{G}$ 的任意两行的线性组合的重量至少是 $2 + 2$,因而重量为 6. 于是, $\bar{G}$ 的两行的线性组合后六个分位上恰有两个 0。这意味着 $\bar{G}$ 的任意三行的线性组合的重量至少是 $3 + 1$,即至少为 6. 因此 $\bar{C}$ 的极小距离为 6. 由此即得 C 是一个 $(11, 3^6, 5)$ 码. 又由 $|B_2(\mathbf{x})| = \sum_{i=0}^{2} \binom{11}{i} 2^i = 3^5$, 知 C 是一个完全码. 这个码叫做**三元 Golay 码**. 已经证明任意 $(11, 3^6, 5)$ 码都与 C 等价(参见[46]).

§ 4.4 由已知码构造新码

许多好码可以通过各种方式修正前面构造的码而得到. 我们

将在这一节给出几个例子．第一个方法是在(3.2.7)中引进的，即加上一个额外分位(称作奇偶校验位)来扩充一个码．其逆过程就是删减一个码，在§4.2中，我们曾用这个方法从扩充码得到二元Golay码．作为另一个例子，我们考虑(4.1.1)中的(9，20，4)码．删减这个码，即去掉每个码字的最后一个符号，我们得到一个(8，20，3)码．在下一章里，我们将看到它的确是个好码．我们注意到，这个码也可以由码字(11010000)，(11100100)和(10101010)的全部循环加上 **0** 和 **1** 得到．

第三个方法是缩短一个码 C．做法是，取出 C 中最后一个分量相同的全部码字，然后去掉它们的最后这个分量．这个过程虽然减少了码的长度和数量，但并不减少极小距离．我们注意到，如果去掉的符号不是0，那么该过程将一个线性码变成一个非线性码(一般而言)．

现在来看一个稍微复杂点的方法．由§4.2扩充二元Golay码 $\bar{C}$ 的构造，我们立即看到，$\bar{C}$ 有一个含有32个码字的子码，这些码字在头八个分位上均为0．同样，如果取 $c_8=1$，并且 c_1 到 c_7 中恰有一个符号为1，则我们找到一个含有32个码字的子码．穷尽全部的可能方式，我们得到 $\bar{C}$ 中一个含有256个码字的子集，其中任意两个码字在头八个分位上至多有两个分量不同．现在，我们从这些码字中去掉头八个分量，其结果是一个二元(16，256，6)码，它是非线性的．这个码叫作Nordstrom-Robinson码．它是§7.4讨论的无限码序列中的第一个码．如果我们先缩短这个码两次，再删减一次，则得到一个(13，64，5)码，记作 Y．这是下一章的一个重要例子．已知 Y 是唯一的，并且如果缩短 Y，则有两种可能结果(J.-M. Goethals 1977；参见[26])．这两个码是：Nadler 码和问题4.7.7中的码．

与扩充二元Golay码的构造类似的一种构造是所谓的 $(\mathbf{u},\mathbf{u}+\mathbf{v})$_构造．设 C_i 是二元 (n, M_i, d_i) 码 $(i=1,2)$．定义

(4.4.1) $$C:=\{(\mathbf{u},\mathbf{u}+\mathbf{v})\mid \mathbf{u}\in C_1, \mathbf{v}\in C_2\},$$

则 C 是一个 $(2n, M_1M_2, d)$ 码，其中 $d:=\min\{2d_1, d_2\}$．要证明

这点，我们考虑码字 $(\mathbf{u}_1, \mathbf{u}_1+\mathbf{v}_1)$ 和 $(\mathbf{u}_2, \mathbf{u}_2+\mathbf{v}_2)$. 如果 $\mathbf{v}_1=\mathbf{v}_2$, $\mathbf{u}_1\neq\mathbf{u}_2$, 则它们的距离至少是 $2d_1$. 如果 $\mathbf{v}_1\neq\mathbf{v}_2$, 则它们的距离是 $w(\mathbf{u}_1-\mathbf{u}_2)+w(\mathbf{u}_1-\mathbf{u}_2+\mathbf{v}_1-\mathbf{v}_2)$ 显然大于 $w(\mathbf{v}_1-\mathbf{v}_2)$, 即至少是 d_2. 作为一个例子，我们取上面构造的 (8, 20, 3)码为 C_2, 再取 C_1 为一个[8, 7]偶重量码，则我们构造出一个 $(16, 5\cdot 2^9, 3)$ 码. 当 $M>5\cdot 2^9$ 时，现在还不知道是否存在 $(16, M, 3)$ 码.

利用 H. J. Helgert 和 R. D. Stinaff 的下述思想(1973; 参见 [34]), 可以构造许多好码. 设 C 是一个极小距离为 d 的二元 $[n, k]$ 码，我们可设 C 的生成矩阵 G 的第一行重量为 d, 譬如说

$$G=\left[\begin{array}{cc|cc}1 & 1\cdots 1 & 0 & 0\cdots 0\\ & G_1 & & G_2\end{array}\right].$$

由 G_2 生成一个码，叫做关于 G 的第一行的剩余码. 它是一个 $[n-d, k-1]$ 码，设 d' 是其极小距离. 由 G 可知，剩余码的每个码字对应于 C 中的两个码字，其中至少有一个在前 d 个位置上重量 $\leqslant \frac{1}{2}d$, 因此 $d'\geqslant \frac{1}{2}d$. 为了说明这个方法，我们来证明不存在具有 Nadler 码参数的线性码. 如果存在一个这样的码，则它有如上的生成矩阵，其中 G_2 生成一个极小距离 $d'\geqslant 3$ 的[7, 4]码. 因此，其剩余码是 Hamming 码. 不失一般性，我们可让 G_2 有 4 行的重量为 3, 于是 G_1 必然有 4 行 (不失一般性) 的重量为 2. 这仅有几种可能性，它们都不能产生 $d=5$ 的码. 即使对于较小的参数值，要找到一个好码也常常是相当困难的. 比如，一个 (10, 38, 4) 码是用相当复杂的方法构造出来的(参见 [46], 第二章，第七节), 而且长期以来都认为它是不能改进的. 最近，M. R. Best (1978; 参见 [8])找到了一个(10, 40, 4)码，我们介绍如下. 在下一章，我们将看到，对于 $n=10$, $d=4$, 这是一个名符其实的最好码[1]! 考虑一个[5, 3] 码 C_1, 其生成矩阵为

1) 码的构造者名叫 M. R. Best, Best 在英文中表示最好的. ——译者注

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix},$$

重复码字两次，我们得到一个最小距离 $d=4$ 的[10, 3]码 C_2. 将(10000 00100)与 C_2 的所有码字相加，则新码不再是线性码，并且不包含 **0**. 将分位从 1 到 10 编号，然后用 S_{10} 的由 (1 2 3 4 5)(6 7 8 9 10)生成的子群的元素置换码字，就得到 40 个码字，它们的极小距离为 4.

§4.5 Reed-Muller 码

现在我们描述一类与有限几何相联系的二元码. D. E. Muller (1954)和 I. S. Reed (1954) 首先研究了这类码. 虽然它们不象后面几章里的一些码好，但在实用中却有易于译码的优点，其译码方法是大数逻辑译码(参见 §3.4) 的一个推广.

可用几种方式表示 Reed-Muller 码的码字. 我们将尝试给出一个统一的处理，以便能看出不同观点间的联系. 作为准备，我们需要一个数论的定理，它已有一个世纪的历史了 (Lucas, 1878).

(4.5.1)定理. 设 p 是一个素数，又设

$$n=\sum_{i=0}^{l} n_i p^i,\quad k=\sum_{i=0}^{l} k_i p^i$$

是 n 和 k 的 p-进制表示(即 $0\leqslant n_i\leqslant p-1$, $0\leqslant k_i\leqslant p-1$)，则

$$\binom{n}{k}\equiv\prod_{i=0}^{l}\binom{n_i}{k_i}\pmod p$$

证明. 我们利用 $(1+x)^p\equiv 1+x^p \pmod p$ 这一事实. 如果 $0\leqslant r<p$, 则

$$(1+x)^{ap+r}\equiv(1+x^p)^a(1+x)^r \pmod p,$$

比较上式两端 x^{bp+s} (这里 $0\leqslant s<p$) 的系数，有

$$\binom{ap+r}{bp+s} \equiv \binom{a}{b}\binom{r}{s} \pmod{p},$$

再由归纳法,即得定理. □

下面的关于多项式重量的定理也是需要的. 设 $q=2^r$, 对任一多项式 $P(x)\in \mathbb{F}_q[x]$, 我们定义 $P(x)$ 的 Hamming 重量 $w(P(x))$ 为 $P(x)$的展开式中非零系数的个数. 设 $c\in \mathbf{F}_q$, $c\neq 0$, 则多项式 $(x+c)^i$, $i\geqslant 0$, 是 $\mathbf{F}_q[x]$ 的一组基.

(4.5.2)定理 (Massey 等,1973; 参见[49]). 设 $P(x)=\sum_{i=0}^{l} b_i(x+c)^i$, 其中 $b_l\neq 0$, 并且设 i_0是使得 $b_i\neq 0$ 的最小指标, 则

$$w(P(x))\geqslant w((x+c)^{i_0}).$$

证明. 若 $l=0$, 则结论显然成立. 我们用归纳法. 假设定理对 $l<2^n$ 成立. 现在设 $2^n\leqslant l<2^{n+1}$, 则有

$$\begin{aligned}P(x) &= \sum_{i=0}^{2^n-1} b_i(x+c)^i + \sum_{i=2^n}^{l} b_i(x+c)^i\\ &= P_1(x)+(x+c)^{2^n}P_2(x)\\ &= (P_1(x)+c^{2^n}P_2(x))+x^{2^n}P_2(x),\end{aligned}$$

其中 $P_1(x)$ 和 $P_2(x)$ 是使定理成立的多项式. 我们区分两种情况:

(i) 若 $P_1(x)=0$, 则 $w(P(x))=2w(P_2(x))$, 又因为 $i_0\geqslant 2^n$, 有

$$\begin{aligned}w((x+c)^{i_0}) &= w((x^{2^n}+c^{2^n})(x+c)^{i_0-2^n})\\ &= 2w((x+c)^{i_0-2^n}),\end{aligned}$$

所以结论成立.

(ii) 若 $P_1(x)\neq 0$, 则对于 $C^{2^n}P_2(x)$ 中的每一项, 如果它消去 $P_1(x)$ 中的一项, 那么 $x^{2^n}P_2(x)$ 中就必有一项不能消去. 因此, $w(P(x))\geqslant w(P_1(x))$, 由归纳假设知定理成立. □

现在我们介绍 Reed-Muller 码的码字的三种表示: (i) $AG(m,2)$ 中子集的特征函数; (ii) 多项式二元展开式的系数; (iii) $\mathbf{F}_2^m$ 上 Bool 函数的真值表.

先给一些符号和定义．考虑 AG$(m, 2)$ 中的点，它们可以视为 $\mathbf{F}_2^m$ 中的列向量，用 $\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{m-1}$ 记其标准基．设 j 的二元表示为 $j=\sum_{i=0}^{m-1} \xi_{ij} 2^i \ (0 \leqslant j < 2^m)$.

定义 $\mathbf{x}_j := \sum_{i=0}^{m-1} \xi_{ij} \mathbf{u}_i$，它表示了 AG$(m, 2)$ 中的一个点，并且 AG$(m, 2)$ 中的所有的点都可以这样得到．设 E 是一个矩阵，其列为 $\mathbf{x}_j \ (0 \leqslant j < 2^m)$．记 $n := 2^m$，则 $m \times n$ 矩阵 E 以 AG$(m, 2)$中的点为其列向量．

(4.5.3)定义．

(i) $A_i := \{\mathbf{x}_j \in \mathrm{AG}(m, 2) \mid \xi_{ij} = 1\}$，即 $A_i (0 \leqslant i < m)$ 是一个 $(m-1)$-维仿射子空间(超平面)；

(ii) $\mathbf{v}_i := E$ 的第 i 行，即 A_i 的特征函数．向量 $\mathbf{v}_i$ 是 $\mathbf{F}_2^n$ 中的元素．如通常一样，AG$(m,2)$ 的特征函数记为 $\mathbf{1} := (1, 1, \cdots, 1)$；

(iii) 如果 $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$ 和 $\mathbf{b} = (b_0, b_1, \cdots, b_{n-1})$ 是 $\mathbf{F}_2^n$ 的元素，定义

$$\mathbf{ab} := (a_0 b_0, a_1 b_1, \cdots, a_{n-1} b_{n-1});$$

(iv) 如果 $S \subset \{0, 1, \cdots, m-1\}$，定义

$$C(S) := \left\{ j = \sum_{i=0}^{m-1} \xi_{ij} 2^i \mid i \notin S \Rightarrow \xi_{ij} = 0 (0 \leqslant i < m) \right\}.$$

(4.5.4)引理． *设 $l = \sum_{i=0}^{m-1} \xi_{il} 2^i$，又设 $i_1, \cdots, i_s$ 是使 $\xi_{il} = 0$ 的 i 值．如果*

$$\mathbf{v}_{i_1} \mathbf{v}_{i_2} \cdots \mathbf{v}_{i_s} = (a_{l,0}, a_{l,1}, \cdots, a_{l,n-1}),$$

则

$$(x+1)^l = \sum_{j=0}^{n-1} a_{l,j} x^{n-1-j}.$$

(这里像通常一样，无因子 $(s=0)$ 时的乘积定义为 $\mathbf{1}$.)

证明．由定理 4.5.1，二项系数$\binom{l}{n-1-j}$为 1 当且仅当对每个使得 $\xi_{il}=0$ 的 i 都有 $\xi_{ij}=1$．由(4.5.3)的 (i)，(ii)和(iii)，我们又有 $a_{l,j}=1$ 当且仅当对 $i=i_1,\cdots,i_s$，$\xi_{ij}=1$． □

下述引理给出了乘积 $\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s}$ 的几何解释．

(4.5.5)引理． 如果 $i_1,i_2,\cdots,i_s$ 互异，则

(i) $\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_s}$ 是 $(m-s)$-平坦 $A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_s}$ 的特征函数，

(ii) 向量 $\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s}$ 在 $\mathscr{R}^{(n)}=\mathbf{F}_2^n$ 中的重量 $w(\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s})$ 是 2^{m-s}，

(iii) $\{\mathbf{x}_j\}$——$\mathscr{R}^{(n)}=\mathbf{F}_2^n$ 的第 j 个基向量——的特征函数是

$$\mathbf{e}_j=\prod_{i=0}^{m-1}\{\mathbf{v}_i+(1+\xi_{ij})\mathbf{1}\},$$

(iv) 乘积 $\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s}$ $(0\leqslant s\leqslant m)$ 是 $\mathscr{R}^{(n)}$ 的基．

证明．

(i) 是(4.5.3)之 (i)—(iii) 的一个推论．

(ii) 由 (i)，重量 $w(\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s})$ 是一个 $(m-s)$-平坦的基数

(iii) 考虑矩阵 E．对每个使得 $\xi_{ij}=0$ 的 i，我们用 $\mathbf{v}_i$ 的补 $\mathbf{v}_i+\mathbf{1}$ 替换 E 的第 i 行 $\mathbf{v}_i$，再将新矩阵的行全部相乘，则由于所有的列只出现一次，所以乘积向量仅在第 j 个分位上为 1．作为一个例子，考虑下表中的 $\{\mathbf{x}_{14}\}$．因为 $14=0+2+2^2+2^3$，所以只有 $i=0$ 时才有 $1+\xi_{ij}=1$（这里 $j=14$）．于是在表中我们对行 $\mathbf{v}_0$ 求补，然后把所有向量相乘，得 $(\mathbf{v}_0+\mathbf{1})\mathbf{v}_1\mathbf{v}_2\mathbf{v}_3$ 是一个仅在第 14 个位置为 1 的行向量．

(iv) 总共有 $\sum_{s=0}^{m}\binom{m}{s}=2^m=n$ 个乘积 $\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s}$．结果可由 (iii) 推得．因为多项式 $(x+1)^l$ 是独立的，我们也可以利用引理 4.5.4． □

下表用来说明引理 4.5.4 和 4.5.5．例如，$\mathbf{v}_0\mathbf{v}_2$ 相应于 $l=15-2^0-2^2=10$，因此 $(x+1)^{10}=x^{10}+x^8+x^2+1$．

$\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_s}$	坐标＝$(x+1)^l$的系数	$l=n-1-\sum 2^{i_\nu}$
$\mathbf{1}$	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	15 = 1111
$\mathbf{v}_0$	0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1	14 = 1110
$\mathbf{v}_1$	0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1	13 = 1101
$\mathbf{v}_2$	0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1	11 = 1011
$\mathbf{v}_3$	0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1	7 = 0111
$\mathbf{v}_0\ \mathbf{v}_1$	0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1	12 = 1100
$\mathbf{v}_0\ \mathbf{v}_2$	0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1	10 = 1010
$\mathbf{v}_0\ \mathbf{v}_3$	0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 1	6 = 0110
$\mathbf{v}_1\ \mathbf{v}_2$	0 0 0 0 0 0 1 1 0 0 0 0 0 0 1 1	9 = 1001
$\mathbf{v}_1\ \mathbf{v}_3$	0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1	5 = 0101
$\mathbf{v}_2\ \mathbf{v}_3$	0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1	3 = 0011
$\mathbf{v}_0\ \mathbf{v}_1\ \mathbf{v}_2$	0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1	8 = 1000
$\mathbf{v}_0\ \mathbf{v}_1\ \mathbf{v}_3$	0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1	4 = 0100
$\mathbf{v}_0\ \mathbf{v}_2\ \mathbf{v}_3$	0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1	2 = 0010
$\mathbf{v}_1\ \mathbf{v}_2\ \mathbf{v}_3$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1	1 = 0001
$\mathbf{v}_0\ \mathbf{v}_1\ \mathbf{v}_2\ \mathbf{v}_3$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1	0 = 0000

(4.5.6)定义. 设 $0 \leqslant r < m$，以乘积 $\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s}$ 为基的、长为 $n=2^m$ 的线性码称为 r 阶二元 Reed-Muller 码(RM 码，记为 $\mathscr{R}(r, m)$).

特别地，$\mathscr{R}(0, m)$ 是重复码. 由引理 4.5.5 (i)，我们看到，若 $\mathbf{x}=(x_0,\cdots,x_{m-1})$ 跑遍 $\mathbf{F}_2^m$，则 Bool 函数 $x_{i_1}\ x_{i_2}\cdots x_{i_s}$ 取值为 1 当且仅当 $x\in A_{i_1}\cap\cdots\cap A_{i_s}$. 因此 $\mathscr{R}(r, m)$ 由 $x_0, x_1, \cdots, x_{m-1}$ 的至多 r 次的多项式的真值序列所组成.

(4.5.7)定理. $\mathscr{R}(r, m)$ 的极小距离为 2^{m-r}.

证明. 由定义和引理 4.5.5 (ii)，$\mathscr{R}(r, m)$ 的极小距离至多为 2^{m-r}，又由引理 4.5.4 和定理 4.5.2，其极小距离至少是 2^{m-r}(也可看问题 4.7.9). □

(4.5.8)定理. $\mathscr{R}(r, m)$ 的对偶码是 $\mathscr{R}(m-r-1, m)$.

证明.

(a) 由定义及乘积 $\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s}$ 的独立性，$\mathscr{R}(r, m)$ 的维数是 $1+\binom{m}{1}+\cdots+\binom{m}{r}$. 于是 $\dim\mathscr{R}(r, m)+\dim\mathscr{R}(m-r-$

$1, m) = n$.

(b) 设 $\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s}$ 和 $\mathbf{v}_{j_1}\cdots\mathbf{v}_{j_t}$ 分别是 $\mathscr{R}(r, m)$ 和 $\mathscr{R}(m-r-1, m)$ 的基向量，则 $s+t<m$. 因此这两个基向量的乘积具有形式 $\mathbf{v}_{k_1}\cdots\mathbf{v}_{k_u}$, 其中 $u<m$. 由引理 4.5.5 (ii)，这个乘积具有偶重量，即原来的两个基向量正交. □

推论. $\mathscr{R}(m-2, m)$ 是一个 $[n, n-m-1]$ 扩充 Hamming 码.

给定一个 RM 码，我们可以选择某些平坦的特征函数作为它的基. 现在我们来证明，对于每一个具有适当维数的平坦，它的特征函数属于某个 RM 码.

(4.5.9)定理. 设 $C=\mathscr{R}(m-l, m)$, A 是 $AG(m, 2)$ 中的一个 l-平坦，则 A 的特征函数属于 C.

证明. 设 $\mathbf{f}=\sum_{j=0}^{n-1} f_j\mathbf{e}_j$ 是 A 的特征函数. 由定义 4.5.3 (iv) 和引理4.5.5 (iii)，我们有

$$\mathbf{e}_j=\sum_{s=0}^{m}\sum_{\substack{(i_1,\cdots,i_s)\\ j\in C(i_1,\cdots,i_s)}}\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_s},$$

因此

$$\mathbf{f}=\sum_{s=0}^{m}\sum_{(i_1,\cdots,i_s)}\left(\sum_{j\in C(i_1,\cdots,i_s)} f_j\right)\mathbf{v}_{i_1}\cdots\mathbf{v}_{i_s},$$

其中上式括号里的和是 A 与 s-平坦

$$L=\{\mathbf{x}_j\in AG(m, 2)\mid j\in C(i_1, \cdots, i_s)\}$$

相交元素的个数. 若 $s>m-l$, 则 $L\cap A$ 或是空集，或是一个维数大于 0 的仿射子空间. 在这两种情形下，$|L\cap A|$ 都是偶数，即括号内之和为 0. □

这个定理和 RM 码的定义表明，一个字属于 $\mathscr{R}(r, m)$ 当且仅当它是一些维数 $\geqslant m-r$ 的仿射子空间的特征函数之和. 采用 Bool 函数的术语，则 $\mathscr{R}(r, m)$ 是 $x_0, x_1, \cdots, x_{m-1}$ 上次数 $\leqslant r$ 的多项式集合.

在 § 3.2 中，利用作用于码字分位的置换，我们给出了等价码的定义．现在我们考虑一个字长为 n 的码 C 以及把 C 中每个码字映到 C 中的置换 $\pi \in S_n$，这些置换构成一个群，叫做 C 的**自同构群**（记为 Aut(C)）．例如，设 C 是一个重复码，那么 $\mathrm{Aut}(C) = S_n$．

(4.5.10)定理． $\mathrm{AGL}(m, 2) \subset \mathrm{Aut}(\mathscr{R}(r, m))$．

证明．这是定理 4.5.9 和下述事实的一个直接推论，即 $\mathrm{AGL}(m, 2)$ 把一个 k-平坦映成一个 k-平坦（对每一个 k）．□

注记． 读者应该注意到，我们把 $\mathrm{AGL}(m, 2)$ 看成是作用在 $\mathrm{AG}(m, 2)$ 上的置换群，而其位置是利用 $\mathrm{AG}(m, 2)$ 中的元素来编号的．

不涉及细节，我们简要地描述 RM 码的一个译码程序，它是大数逻辑译码的推广．设 $C = \mathscr{R}(r, m)$，由定理 4.5.8 和 4.5.9，$\mathrm{AG}(m, 2)$ 中任意 $(r+1)$-平坦的特征函数都是 C 的奇偶校验向量．给定一个 r-平坦 A，则存在 $2^{m-r} - 1$ 个不同的包含 A 的 $(r+1)$-平坦．一个不在 A 中的点恰属于这些 $(r+1)$-平坦中的某一个，这些 $(r+1)$-平坦中的每一个都包含 A 并且包含与 A 中点数相同的不在 A 中的点．

现在，我们观察奇偶校验的结果．设接收到的字含有少于 $2^{m-r} - 1$ 个差错（见定理 4.5.7），又设有 t 个奇偶校验不为 0，对此有两种可能的解释：

(i) 由 A 的位置中含有奇数个差错引起，这些差错被校验集余下位置中的奇数个差错抵消了 $2^{m-r} - 1 - t$ 次．

(ii) A 的位置中含有偶数个差错，但对上述的 t 个校验方程，在余下的位置中有奇数个差错．

由极大似然法，如果 $t < 2^{m-r}$，则 (ii) 比 (i) 更有可能；否则 (i) 更有可能．这意味着我们有可能决定任意一个 r-平坦的位置差错个数之奇偶性．然后，对 $(r-1)$-平坦用类似的方法做同样的事情．如此下去，经过 $r+1$ 步即可找出全部差错位置．这个过程叫做**大数逻辑译码**．

§ 4.6 评　　注

关于航海者号在考察中使用 Hadamard 码的细节，我们建议参阅[56].

Golay 码是由 M. J. E. Golay 在 1947 年用不同于本书的方法构造出来的. 对这些码更多的讨论以及它们与组合理论的若干联系，我们建议参阅 J. Cameron 和 J.H. van Lint 的书[11]或[46].

对与 § 4.4 有关的内容感兴趣的读者，可参考文献[64]和[65]. RM 码的编码和译码的更多的讨论，可参阅[2]或[46].

§ 4.7 问　　题

4.7.1. 设 $n = 2^m$，证明 Reed-Muller 码 $\mathscr{R}(1, m)$ 是一个长为 n 的 Hadamard 码.

4.7.2. 证明三元 Golay 码中重为 5 的码字有 132 个. 对于每个重为 5 的码的偶 $\{x, 2x\}$，考虑使得 $x_i \neq 0$ 的位置子集，证明这 66 个集合构成一个 $4-(11, 5, 1)$ 设计.

4.7.3. 设 S 是 11 阶 Paley 矩阵. $A = \frac{1}{2}(S + I + J)$. 考虑 A 的行，A 的 55 个互异的两行之和以及这些行的补. 证明这是一个 $(11, 132, 3)$ 码.

4.7.4. 构造一个 $(17, 36, 8)$ 码.

4.7.5. 设 A 是问题 4.7.3 中的矩阵. 定义

$$G := \left[\begin{array}{c|c|ccc} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I_{12} & 1 & & A & \\ & \vdots & & & \\ & 1 & & & \end{array}\right].$$

证明G生成的码等价于扩充二元 Golay 码.

4.7.6. 证明：如果存在一个 d 为偶数的二元 (n, M, d) 码，则有一个全部字为偶数的 (n, M, d) 码.

4.7.7. 设 3×3 矩阵 I, J 和 P 如同(4.1.1)，定义

$$A:=\begin{bmatrix} J-I & I & I & I \\ I & J-I & I & I \\ I & I & J-I & I \\ I & I & I & J-I \end{bmatrix},$$

$$B:=\begin{bmatrix} J & P & I & P^2 \\ P & J & P^2 & I \\ I & P^2 & J & P \\ P^2 & I & P & J \end{bmatrix},$$

$$C:=(J-I \quad J-I \quad J-I \quad J-I),$$

$$D:=\begin{bmatrix} 000 & 111 & 111 & 111 \\ 111 & 000 & 111 & 111 \\ 111 & 111 & 000 & 111 \\ 111 & 111 & 111 & 000 \end{bmatrix}.$$

证明，$\mathbf{0}$ 和 A, B, C, D 的行都是某个 $(12, 35, 5)$码的码字.

4.7.8. 设H是(1.3.9)的 Hadamard 矩阵 H_{12}, $A:=H-I$, $G:=(I, A)$. 证明 G 是一个极小距离为 9 的三元 $[24, 12]$ 码的生成矩阵.

4.7.9. 设 $C_1=\mathscr{R}(r+1, m)$, $C_2=\mathscr{R}(r, m)$. 证明(4.4.1)的 $(\mathbf{u}, \mathbf{u}+\mathbf{v})$-构造产生 $C=\mathscr{R}(r+1, m+1)$. 利用这个结果给出定理4.5.7的另一证明.

4.7.10. (i) 设 $n=2^m$, 对 $\mathbf{x}\in\mathbb{F}_2^n$, 定义 $\mathbf{x}^*\in\{1, -1\}^n$ 为用 -1 代替 $\mathbf{x}$ 中的 0 而得到的向量. 在问题 4.7.1 中我们看到，这个映射运用到 $\mathscr{R}(1, m)$, 则得到向量 $\pm\mathbf{a}_1$, $\pm\mathbf{a}_2$, $\cdots$, $\pm\mathbf{a}_n$, 这里 $\mathbf{a}_i$ 都是某个 Hadamard 矩阵的行. 利用这点证明：如果 $\mathbf{x}\in\mathbb{F}_2^n$, 则存在码字 $\mathbf{c}\in\mathscr{R}(1, m)$, 使得 $d(\mathbf{x}, \mathbf{c})\leqslant(n-\sqrt{n})/2$.

(ii) 如果 $m=2k$，$\mathbf{x}$ 是 $\mathscr{R}(2,m)$ 中相应于 Bool 函数 $x_1x_2+x_3x_4+\cdots+x_{2k-1}x_{2k}$ 的字，证明 $d(\mathbf{x},\mathbf{c})\geq(n-\sqrt{n})/2$，对于全部 $\mathbf{c}\in\mathscr{R}(1,m)$．(换句话说，$\mathscr{R}(1,2k)$ 的覆盖半径是 $2^{2k-1}-2^{k-1}$．)

4.7.11. 设H是三元[4，2] Hamming 码的奇偶校验矩阵，令 I 和 J 分别是 4×4 单位矩阵和全 1 矩阵，证明

$$G:=\begin{bmatrix} J-I & I & I \\ 0 & H & -H \end{bmatrix}$$

生成一个 $d=6$ 的 [12，6] 码 C，即一个等价于扩充三元 Golay 码的码．

第五章 码的界

§ 5.1 引言；Gilbert 界

在这一章中，我们将对这样的码感兴趣，对于给定的码字长和码的极小距离，码含有尽可能多的码字，而对这些码的实用性、它们的编码和译码等问题则不加考虑．我们还是以 q 个符号的集Q作为字母表，并定义 $\theta:=(q-1)/q$．记号与 § 3.1 相同．假设 q 已取定，则一个 $(n, *, d)$ 码是指一个长为 n，极小距离为 d 的码．我们对码字的最大数目（即能放在＊处的最大的 M）感兴趣．如果一个 (n, M, d) 码不含在任意 $(n, M+1, d)$ 码中，则称它为**极大的**．

(5.1.1)定义． $A(n, d):=\max\{M \mid$ 存在一个 (n, M, d) 码$\}$．码C称为**最优的**，如果 $|C|=A(n, d)$．

有些作者把极小距离 $d=n-k+1$ 的 $[n, k]$ 码称为"最优的"（见问题 3.7.2）．这样的码在 (5.1.1) 的意义下是最优的（参见(5.2.2)）．通常$[n, k, n-k+1]$码称为**极大距离可分码** （MDS码）．

数 $A(n, d)$ 的研究被认为是组合编码理论的中心问题．在第二章中，我们已经看到好码是长的，或者更确切地说，在给定差错概率为 p 的信道上，通过考察一列长度递增的码，我们可以降低差错概率．显然，在一个接收字里差错的平均数是 np．因此，如果我们希望纠正这些差错，码的极小距离 d 至少应与 $2np$ 增长得一样快．这就解释了下述定义中所给的数 $\alpha(\delta)$ 的重要性．

(5.1.2)定义．

$$\alpha(\delta):=\limsup_{n\to\infty} n^{-1}\log_q A(n, \delta n).$$

在第二章，我们讨论了具有给定信息率的一些好码．在那时，

我们问的是 d/n（作为 n 的函数）有多大. 由 (5.1.2)，这意味着我们对逆函数 $\alpha^{\leftarrow}(R)$ 有兴趣.

一般来说，函数 A 和 α 都是未知的，我们将研究它们的上界和下界，以及 $A(n, d)$ 的一些特殊值. 码的扩充、缩短和删减（见 § 4.4）等技巧将经常使用，由它们直接可推出下述定理.

(5.1.3)定理. 对于二元码，有

$$A(n, 2l-1) = A(n+1, 2l).$$

我们请读者回忆 § 3.1 中球 $B_r(\mathbf{x})$ 的定义，并再定义

$$(5.1.4) \qquad V_q(n, r) := |B_r(\mathbf{x})| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

（参见(3.1.6)）.

为了研究函数 α，我们需要推广(1.4.4)定义的熵函数. 设 $\theta := (q-1)/q$，我们如下定义 $[0, \theta]$ 上的熵函数 H_q:

$$(5.1.5) \qquad \begin{aligned} H_q(0) &:= 0 \\ H_q(x) &:= x\log_q(q-1) - x\log_q x \\ &\quad - (1-x)\log_q(1-x), \text{ 对 } 0 < x \leqslant \theta. \end{aligned}$$

注意，当 x 从 0 变到 θ 时，$H_q(x)$ 从 0 增加到 1.

(5.1.6)定理. 设 $0 \leqslant \lambda \leqslant \theta$，$q \geqslant 2$，则

$$\lim_{n\to\infty} n^{-1}\log_q V_q(n, \lfloor \lambda n \rfloor) = H_q(\lambda).$$

证明. 对 $r = \lfloor \lambda n \rfloor$，在 (5.1.4) 右边的和式中，最后一项是最大的. 因此

$$\begin{aligned} \binom{n}{\lfloor \lambda n \rfloor}(q-1)^{\lfloor \lambda n \rfloor} &\leqslant V_q(n, \lfloor \lambda n \rfloor) \\ &\leqslant (1 + \lfloor \lambda n \rfloor)\binom{n}{\lfloor \lambda n \rfloor}(q-1)^{\lfloor \lambda n \rfloor}. \end{aligned}$$

对上式先取对数，再用 n 除，然后仿定理 1.4.5 的证明，即可得所要的结果.

在结束本节之前，我们来讨论已知的 $A(n, d)$ 的最好的下界及相应的 $\alpha(\delta)$ 的界. 实际上 $\alpha(\delta)$ 是很可能达到这个下界的. 然而令人惊奇的是，这个界的证明却完全是平凡的.

(5.1.7)定理. 对于 $n \in \mathbf{N}$, $d \in \mathbf{N}$, $d \leqslant n$,我们有

$$A(n, d) \geqslant q^n / V_q(n, d-1).$$

证明. 设 C 是一个极大的 (n, M, d) 码. 即 Q^n 中没有字与 C 中的所有字的距离大于或等于 d. 换句话,球 $B_{d-1}(\mathbf{c})$, $\mathbf{c} \in C$, 覆盖了 Q^n. 因此, 它们的"体积"之和 $|C| V_q(n, d-1)$ 超过了 $q^n = |Q|^n$. □

这个证明告诉我们,一个至少含有 $q^n / V_q(n, d-1)$个码字的码可以很简单地构造出来: 从任一个字 $\mathbf{c}_0$ 开始, 相继加上一些新字使它们与先前已选好的字的距离至少是 d, 直到码成为极大的时候为止. 这样的码没有什么结构. 奇怪的是, 要求 C 是线性的并不是本质上的限制,正如下面的定理所表明的那样.

(5.1.8)定理. 如果 $n \in \mathbf{N}$, $d \in \mathbf{N}$, $k \in \mathbf{N}$ 满足 $V_q(n, d-1) < q^{n-k+1}$,则存在一个 $[n, k, d]$ 码.

证明. $k = 0$ 时定理是平凡的. 设 C_{k-1} 是一个 $[n, k-1, d]$ 码, 因为 $|C_{k-1}| V_q(n, d-1) < q^n$, 所以它不是极大码. 因此,存在字 $\mathbf{x} \in Q^n$, 它与 C_{k-1} 中所有字的距离 $\geqslant d$. 令 C_k 是由 C_{k-1} 和$\{\mathbf{x}\}$张成的码. 设 $\mathbf{z} = a\mathbf{x} + \mathbf{y}$(这里 $0 \neq a \in Q$, $\mathbf{y} \in C_{k-1}$)是 C_k 中的一个码字,则

$$\begin{aligned} w(\mathbf{z}) &= w(a^{-1}\mathbf{z}) = w(\mathbf{x} + a^{-1}\mathbf{y}) \\ &= d(\mathbf{x}, -a^{-1}\mathbf{y}) \geqslant d. \end{aligned}$$ □

问题 3.7.14 中的码是定理 5.1.8 的一个例子.

例. 设 $q = 2$, $n = 13$, $d = 5$, 则由(5.1.4)我们有 $V_2(13, 4) = 1093$, 因此 $A(13, 5) \geqslant \lceil 8192/1093 \rceil = 8$. 事实上, 定理 5.1.8 保证了$[13, 3, 5]$码的存在性. 显然这不是一个很好的码, 因为由定理 4.5.7, 删减 $\mathscr{R}(1, 4)$ 三次, 我们即可得到一个 $[13, 5, 5]$ 码. 而事实上, § 4.4 中的码 $\mathbf{Y}$ 是更好的非线性码,它是一个$(13, 64, 5)$码. 这个例子说明了寻找 $A(n, d)$ 的界的一个方法, 即构造好码. 我们有 $A(13, 5) \geqslant 64$.

定理 5.1.7 中的界称为 Gilbert 界(或 Gilbert-Varshamov 界). 现在我们考虑 α 的相应的界.

(5.1.9)定理（渐近 Gilbert 界）．如果 $0 \leqslant \delta \leqslant \theta$，则

$$\alpha(\delta) \geqslant 1 - H_q(\delta).$$

证明．由 (5.1.7)和(5.1.6)，我们有

$$\alpha(\delta) = \limsup_{n\to\infty} n^{-1}\log_q A(n, \delta n) \geqslant \lim_{n\to\infty}\{1 - n^{-1}\log_q V_q(n, \delta n)\}$$
$$= 1 - H_q(\delta). \qquad \square$$

§5.2 上　　界

在这一节，我们讨论 $A(n, d)$ 的一些比较容易得到的上界．在过去的几年里，通过应用更复杂的方法，得到了一些更好的界．这些将在 § 5.3 中讨论．

删减一个 (n, M, d) 码 $d-1$ 次，就得到一个 $(n-d+1, M, 1)$ 码，即删减后的M个码字是不同的．因此 $M \leqslant q^{n-d+1}$．这就证明了下述定理，称为 Singleton 界．

(5.2.1)定理．对于 $q, n, d \in \mathbf{N}$, $q \geqslant 2$，我们有

$$A(n, d) \leqslant q^{n-d+1}.$$

(5.2.2)推论．对于 $\mathbf{F}_q$ 上的一个 $[n, k]$ 码，我们有 $k \leqslant n-d+1$．

达到这个界的码叫做 MDS 码(参看问题 3.7.2)．

例．设 $q=2$, $n=13$, $d=5$，则有 $A(13, 5) \leqslant 512$．

定理 5.2.1 的渐近形式如下：

(5.2.3)定理．对于 $0 \leqslant \delta \leqslant 1$，我们有 $\alpha(\delta) \leqslant 1-\delta$．

下一个界是通过计算两个互异码字间的平均距离的最大可能而得到的．假设C是 (n, M, d) 码，我们把C中的码字列成一张表，考虑其中一列．设Q的第 j 个符号 $(0 \leqslant j \leqslant q-1)$ 在这个列中出现 m_j 次，则这一列对所有有序互异码字间的距离之和的贡献是 $\sum_{j=0}^{q-1} m_j(M-m_j)$，因为 $\sum_{j=0}^{q-1} m_j = M$，利用 Cauchy-Schwarz 不等式，我们有

$$\sum_{j=0}^{q-1} m_j(M - m_j) = M^2 - \sum_{j=0}^{q-1} m_j^2$$

$$\leqslant M^2 - q^{-1}\left(\sum_{j=0}^{q-1} m_j\right)^2 = \theta M^2.$$

因为我们的表共有 n 列，C 中码字的有序对有 $M(M-1)$ 个，故有

$$M(M-1)d \leqslant n\theta M^2.$$

这就证明了 Plotkin 界.

(5.2.4)定理. 对于 $q, n, d \in \mathrm{N}$，$q \geqslant 2$，$\theta = 1 - q^{-1}$，有

$$A(n, d) \leqslant \frac{d}{d - \theta n}，只要\ d > \theta n.$$

例. (a) 设 $q = 2$，$n = 13$，$d = 5$，则 $\theta = \frac{1}{2}$. 为了应用定理 5.2.4，我们考虑一个 $(13, M, 5)$ 码，将它缩短 4 次则可以得到一个$(9, M', 5)$码，其中 $M' \geqslant 2^{-4}M$. 由 Plotkin 界，$M' \leqslant 5/\left(5 - 4\frac{1}{2}\right) = 10$. 因此 $M \leqslant 160$，即 $A(13.5) \leqslant 160$. 一个更好的界可如下得到：先应用定理 5.1.3，得到 $A(13, 5) = A(14, 6)$，再重复上述论证，就有 $A(14, 6) \leqslant 2^3 \cdot 6/\left(6 - 5\frac{1}{2}\right) = 96$.

(b) 设 $q = 3$，$n = 13$，$d = 9$，则 $\theta = \frac{2}{3}$. 对于三元码，由 Plotkin 界可导出 $A(13, 9) \leqslant 27$. 考虑三元 Hamming 码(参见(3.3.1))的对偶码，它的生成矩阵为

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}.$$

这个矩阵以 PG(2, 3) 的点为列向量，$(a_1, a_2, a_3)G$ 中分量为零的位置相应于 PG(2, 3) 在投影直线 $a_1x_1 + a_2x_2 + a_3x_3 = 0$ 上的点. 即，如果 $\mathbf{a} \neq \mathbf{0}$，那么恰好存在 4 个这样的位置. 因此，每

个非零码字的重量为 9，从而任意两个互异码字的距离为 9. 于是，这是一个使定理 5.2.4 取等式的线性码.

从定理 5.2.4 的证明，我们可以看到，只有当全部互异码字对具有相同的距离时，等式才可能成立. 这样的码叫做**等距码**.

我们再给出一个渐近结果.

(5.2.5)定理(渐近 Plotkin 界). 我们有

$$\alpha(\delta) = 0, \text{ 若 } \theta \leqslant \delta \leqslant 1,$$

$$\alpha(\delta) \leqslant 1 - \delta/\theta, \text{ 若 } 0 \leqslant \delta < \theta.$$

证明. 第一个结论是定理 5.2.4 的平凡推论. 为证第二个结论，我们定义 $n' := \lfloor (d-1)/\theta \rfloor$，则 $1 \leqslant d - \theta n' \leqslant 1 + \theta$. 将一个 (n, M, d) 码缩短为一个(n', M', d)码，则 $M' \geqslant q^{n'-n}M$，又由定理 5.2.4，有 $M' \leqslant d/(d - \theta n') < d$. 因此，$M < dq^{n-n'}$. 由此及 $n'/n \to \delta/\theta (n \to \infty)$ 和 $d = \delta n$，我们得到 $\alpha(\delta) \leqslant 1 - \delta/\theta$. □

下面对线性码给出的界是由 J. H. Griesmer (1960)发现的，这个界渐近等价于 Plotkin 界，但在某些情况下它更好些. 虽然证明是初等的，这个界却常常是最佳的. 我们的证明与 § 4.4 中讨论的 Helgert 和 Stinaff 的方法基于一样的思想. 设 G 是一个$[n, k, d]$码的生成矩阵. 可以设 G 的第一行的重量是 d，事实上，不失一般性，我们可以假设它为$(11\cdots10\cdots0)$，其中前 d 个分量为 1. 其它任意一行在前 d 个分位上至少有 $\lceil d/q \rceil$ 个相同. 因此，关于第一行的剩余码是一个 $[n-d, k-1, d']$ 码，其中 $d' \geqslant \lceil d/q \rceil$. 利用归纳法，我们得到下述定理.

(5.2.6)定理 (Griesmer 界). 对于 $\mathbf{F}_q$ 上的一个 $[n, k, d]$ 码，我们有

$$n \geqslant \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

例. (a) 设 $q = 2$，$n = 13$，$d = 5$. 因为 $\sum_{i=0}^{3} \lceil 5/2^i \rceil = 13$，

我们发现一个 $[13, k, 5]$ 码必须满足 $k \leqslant 6$. §4.4 中的码Y有 64 个码字，但它不是线性的. 事实上，不存在一个$[13,6,5]$码. 若不然，则存在一个 $[12, 5, 5]$ 码，这与 §4.1 中的分析相矛盾. 于是，在这里 Griesmer 界不可达到.

(b) 设 $q = 3$, $n = 14$, $d = 9$. 由 $\sum_{i=0}^{3} \lceil 9/3^i \rceil = 14$ 可知，三元 $[13, k, 9]$ 码满足 $k \leqslant 4$. 这种码的缩短变形类似于定理 5.2.4 后面的例 (b). 假设存在这样的码，如前，无妨假设重量为 9 的字 $(11\cdots10\cdots0)$ 是其生成矩阵的第一行. 于是，同 Griesmer 界的证明一样，剩余码是一个三元 $[5, 3, 3]$ 码. 不失一般性，设它的生成矩阵为

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & a & b \\ 0 & 0 & 1 & c & d \end{bmatrix},$$

其中 a, b, c, d 非 0.

显然，$a \neq b$, $c \neq d$, 因此存在第二行和第三行的一个组合，使其重量为 2. Griesmer 界又不可达到.

(3.1.6)的下述推广是最容易理解的界之一，它叫做 Hamming 界或球覆盖界.

(5.2.7)定理. 如果 $q, n, e \in \mathbb{N}$, $q \geqslant 2$, $d = 2e + 1$, 则

$$A(n, d) \leqslant q^n / V_q(n, e).$$

证明. 当 $\mathbf{c}$ 跑遍一个 $(n, M, 2e + 1)$ 码时，球 $B_e(\mathbf{c})$ 两两不交，因此有 $M \cdot V_q(n, e) \leqslant q^n$. □

例. 设 $q = 2$, $n = 13$, $d = 5$, 则由 $V_2(13, 2) = 1 + 13 + 78 = 92$, 我们得到 $A(13, 5) \leqslant \lfloor 2^{13}/92 \rfloor = 89$.

我们已经定义使得 (5.2.7) 中等式成立的码叫做完全码，在第七章，我们还将回到这个问题.

(5.2.8)定理(渐近 Hamming 界). 我们有

$$\alpha(\delta) \leqslant 1 - H_q\left(\frac{1}{2}\delta\right).$$

证明. $A(n, \lceil \delta n \rceil) \leqslant A\left(n, 2\left\lfloor \frac{1}{2}\delta n \right\rfloor - 1\right) \leqslant q^n / V_q\left(n, \frac{1}{2}\lceil \delta n \rceil - 1\right)$,由引理 5.1.6 知定理成立. □

现在我们讨论一个证明起来稍微困难些的上界，在很长的一段时间里,它是已知的最好上界. 由 Plotkin 界的证明,我们可以清楚地看到,如果码字间的距离不全接近平均距离,则界不可能是好的. 下面的出自 P. Elias 的思想给出了一个更强的结果. 我们将证明 Plotkin 界的方法应用于 Q^n 中适当选择的球中码字的集合. 下面的引理表明如何选择这个球.不失一般性,我们取 $Q = \mathbb{Z}/q\mathbb{Z}$.

(5.2.9)引理. 若 A 和 C 是 Q^n 的子集,则有 $\mathbf{x} \in Q^n$ 使得

$$\frac{|(\mathbf{x} + A) \cap C|}{|A|} \geqslant \frac{|C|}{q^n}.$$

证明. 选取 $\mathbf{x}_0$, 使 $|(\mathbf{x}_0 + A) \cap C|$ 最大,则

$$\begin{aligned} |(\mathbf{x}_0 + A) \cap C| &\geqslant q^{-n} \sum_{\mathbf{x} \in Q^n} |(\mathbf{x} + A) \cap C| \\ &= q^{-n} \sum_{\mathbf{x} \in Q^n} \sum_{\mathbf{a} \in A} \sum_{\mathbf{c} \in C} |\{\mathbf{x} + \mathbf{a}\} \cap \{\mathbf{c}\}| \\ &= q^{-n} \sum_{a \in A} \sum_{\mathbf{c} \in C} 1 = q^{-n}|A||C|. \end{aligned}$$ □

设 C 是一个 (n, M, d) 码, A 是 $B_r(\mathbf{0})$. 不失一般性，我们可以假设引理中的点 $\mathbf{x}_0$ 是 $\mathbf{0}$. 考虑码 $A \cap C$,这是一个 (n, K, d) 码，其中 $K \geqslant MV_q(n, r)/q^n$. 我们以这个码的码字为行做一个 $K \times n$ 矩阵,用 m_{ij} 记这个矩阵的第 i 列中符号 j 的个数,则有

(i) $$\sum_{j=0}^{q-1} m_{ij} = K,$$

并且,因为这个矩阵的行重量至多是 r, 有

(ii) $$\sum_{i=1}^{n} m_{i0} =: S \geqslant K(n - r),$$

因此有

(iii) $\sum_{j=1}^{q-1} m_{ij}^2 \geqslant (q-1)^{-1}\left(\sum_{j=1}^{q-1} m_{ij}\right)^2 = (q-1)^{-1}(K-m_{i0})^2$,

以及

(iv) $$\sum_{i=1}^{n} m_{i0}^2 \geqslant n^{-1}\left(\sum_{i=1}^{n} m_{i0}\right)^2 = n^{-1}S^2.$$

我们再来计算由矩阵的行组成的所有有序对的矩距离之和，由 (i) 到 (iv) 有：

$$\sum_{i=1}^{n}\sum_{j=0}^{q-1} m_{ij}(K-m_{ij}) = nK^2 - \sum_{i=1}^{n}\left(m_{i0}^2 + \sum_{j=1}^{q-1} m_{ij}^2\right)$$

$$\leqslant nK^2 - (q-1)^{-1}\sum_{i=1}^{n}(qm_{i0}^2 + K^2 - 2Km_{i0})$$

$$\leqslant nK^2 - (q-1)^{-1}(qn^{-1}S^2 + nK^2 - 2KS).$$

在上面的不等式中代入 $S \geqslant K(n-r)$，并取 $r \leqslant \theta n$，则 $S \geqslant q^{-1}nK$。我们有

$$\sum_{i=1}^{n}\sum_{j=0}^{q-1} m_{ij}(K-m_{ij}) \leqslant K^2 r(2-(r/\theta n)).$$

因为行的有序对共有 $K(K-1)$ 个，所以

$$K(K-1)d \leqslant K^2 r(2 - r\theta^{-1}n^{-1}).$$

这就证明了下列引理。

(5.2.10) 引理. 如果一个 (n, K, d) 码的全部重量 $\leqslant r \leqslant \theta n$，则

$$d \leqslant \frac{Kr}{K-1}\left(2 - \frac{r}{\theta n}\right).$$

(5.2.11) 定理 (Elias 界). 设 $q, n, r \in \mathrm{N}$, $q \geqslant 2$, $\theta = 1 - q^{-1}$. 再假设 $r \leqslant \theta n$, $r^2 - 2\theta nr + \theta nd > 0$，则

$$A(n, d) \leqslant \frac{\theta nd}{r^2 - 2\theta nr + \theta nd} \cdot \frac{q^n}{V_q(n, r)}.$$

证明. 从引理 5.2.9，我们看到一个 (n, M, d) 码有一个子码，它有 $K \geqslant MV_q(n, r)/q^n$ 个码字，并且这些码字全部含在某个 $B_r(\mathbf{x})$ 中。于是，我们就可以应用引理 5.2.10，得到

$$q^{-n}MV_q(n, r) \leqslant K \leqslant \frac{\theta nd}{r^2 - 2\theta nr + \theta nd}.$$ □

注意,若 $r = \theta n$, $d > \theta n$, 则得到 Plotkin 界.

例. 设 $q = 2$, $n = 13$, $d = 5$, 则 $\theta = \frac{1}{2}$. 估计 (5.2.11) 中的 $A(14, 6)$, 可得最佳结果. 这个结果是

$$A(13, 5) = A(14, 6) \leqslant \frac{42}{r^2 - 14r + 42} \cdot \frac{2^{14}}{\sum\limits_{i<r} \binom{14}{i}},$$

所以,最好的选择是 $r = 3$, 此时 $A(13, 5) \leqslant 162$.

例中的结果不如早期估计的好. 不过, 渐近 Elias 界却是本节中最好的结果.

(5.2.12)定理(渐近 Elias 界). 我们有

$$\alpha(\delta) \leqslant 1 - H_q(\theta - \sqrt{\theta(\theta - \delta)}), \quad \text{若 } 0 \leqslant \delta < \theta,$$
$$\alpha(\delta) = 0, \quad \text{若 } \theta \leqslant \delta < 1.$$

证明. 定理的第二部分由定理 5.2.5 推出. 现在假设 $0 \leqslant \delta \leqslant \theta$, 选取 $0 \leqslant \lambda < \theta - \sqrt{\theta(\theta - \delta)}$, 并令 $r = \lfloor \lambda n \rfloor$, 则 $\theta\delta - 2\theta\lambda + \lambda^2 > 0$. 由定理 5.2.11 及 $d = \lfloor \delta n \rfloor$, 我们有

$$n^{-1}\log_q A(n, \delta n) \leqslant n^{-1}\log_q\left(\frac{\theta nd}{r^2 - 2\theta nr + \theta nd} \cdot \frac{q^n}{V_q(n, r)}\right)$$
$$\sim n^{-1}\left\{\log_q\left(\frac{\theta\delta}{\lambda^2 - 2\theta\lambda + \theta\delta}\right) + n - nH_q(\lambda)\right\}$$
$$\sim 1 - H_q(\lambda), \ (n \to \infty).$$

因此, $\alpha(\delta) \leqslant 1 - H_q(\lambda)$. 由于对每个 $\lambda < \theta - \sqrt{\theta(\theta - \delta)}$ 这都成立,所以即得结论.

下一个界也是基于考察码字子集的思想,这时,我们研究具有固定重量 w 的码字.

首先, 我们必须研究一些与 $A(n, d)$ 相似的数. 我们限定 $q = 2$.

(5.2.13)定义. 在长为 n, 极小距离 $\geqslant d$ 的所有二元码中, 重量为

w 的码字的最大个数记为 $A(n, d, w)$。

(5.2.14) 引理. 我们有

$$A(n, 2k-1, w) = A(n, 2k, w) \leqslant \left\lfloor \frac{n}{w} \left\lfloor \frac{n-1}{w-1} \right\lfloor \cdots \left\lfloor \frac{n-w+k}{k} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor.$$

证明．因为重量相同的码字间的距离为偶数，所以 $A(n, 2k-1, w) = A(n, 2k, w)$. 假设码 C 满足我们的条件，且 $|C| = K$，以 C 中的码字为行做一矩阵，则它的每一列至多含有 $A(n-1, 2k, w-1)$ 个 1. 因此，$Kw \leqslant nA(n-1, 2k, w-1)$，即

$$A(n, 2k, w) \leqslant \left\lfloor \frac{n}{w} A(n-1, 2k, w-1) \right\rfloor.$$

由于 $A(n, 2k, k-1) = 1$，故结论可由归纳法得到. □

这个引理表明了如何估计数 $A(n, d, w)$，我们可以用这个数来估计 $A(n, d)$，就象在 Hamming 界的下列推广中所示，这个推广称为 Johnson 界.

(5.2.15) 定理. 设 $q = 2$, $n, e \in \mathbb{N}$, $d = 2e+1$，则

$$A(n, d) \leqslant \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i} + \dfrac{\binom{n}{e+1} - \binom{d}{e} A(n, d, d)}{\left\lfloor \frac{n}{e+1} \right\rfloor}}.$$

证明．证明思想与 Hamming 界的证明是一样的．设 $\{0, 1\}^n$ 中有 N_{e+1} 个字与 (n, M, d) 码 C 的距离为 $e+1$，则

$$M \cdot \sum_{i=0}^{e} \binom{n}{i} + N_{e+1} \leqslant 2^n.$$

为了估计 N_{e+1}，我们考虑一个任意的码字 $\mathbf{c}$，不失一般性，可设 $\mathbf{c}$ 为 $\mathbf{0}$。于是 C 中重量为 d 的码字个数至多为 $A(n, d, d)$，这些码字中的每一个都与 $\binom{d}{e}$ 个重量为 $e+1$ 的字距离为 e。因为共有

$\binom{n}{e+1}$个重为 $e+1$ 的字，则其中与 C 距离为 $e+1$ 的字至少有$\binom{n}{e+1}-\binom{d}{e}A(n,d,d)$ 个．让 $\mathbf{c}$ 跑遍 C 的所有码字，我们计算出$\{0,1\}^n$ 中有 $M\left\{\binom{n}{e+1}-\binom{d}{e}A(n,d,d)\right\}$个字到 C 的距离为 $e+1$．这些字中的每一个被计算了多少次呢？任取其中之一，不失一般性，仍设为 $\mathbf{0}$．与 $\mathbf{0}$ 的距离为 $e+1$ 的两个码字之间的距离 $\geqslant 2e+1$ 的充分必要条件是它们在相异的位置上为 1．因此，这种码字的个数至多为 $\left\lfloor\frac{n}{e+1}\right\rfloor$．这就给出了所要的 N_{e+1} 的估计． □

由引理 5.2.14，我们看到，若取 $k=e+1$，$w=2e+1$，则

$$A(n,d,d)\leqslant\binom{n}{e}\left\lfloor\frac{n-e}{e+1}\right\rfloor,$$

代入定理 5.2.15，则证明了码 C 满足

$$(5.2.16)\quad |C|\left\{\sum_{i=0}^{e}\binom{n}{i}+\frac{\binom{n}{e}}{\left\lfloor\frac{n}{e+1}\right\rfloor}\left(\frac{n-e}{e+1}-\left\lfloor\frac{n-e}{e+1}\right\rfloor\right)\right\}\leqslant 2^n,$$

这是 Johnson 界的原始形式．

例．设 $q=2$，$n=13$，$d=5$（即 $e=2$），则 $A(13,5,5)\leqslant\left\lfloor\frac{13}{5}\left\lfloor\frac{12}{4}\left\lfloor\frac{11}{3}\right\rfloor\right\rfloor\right\rfloor=23$，再由 Johnson 界，有

$$A(13.5)\leqslant\left\lfloor\frac{2^{13}}{1+13+78+\frac{286-10.23}{4}}\right\rfloor=77.$$

对于 $n=13$，$q=2$，$d=5$，这是迄今为止的最好结果；只有利用下一节的强有力的方法，我们才能求出 $A(13.5)$ 的真实值．

§ 5.3 线性规划界

现在已知的许多关于 $A(n, d)$ 的界的最好结果都基于 P. Delsarte (1973)所发展的方法，其思想是推导出一些与 MacWilliam 恒等式(定理 3.5.3) 有密切联系的不等式，然后利用线性规划的技术分析这些不等式. 这一节主要依赖 Krawtchouk 多项式的一些性质.

为了避免繁琐的符号，我们假定 q 和 n 已经取定. 定义

$$K_k(x) := \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j},$$

其中

$$\binom{x}{j} := \frac{x(x-1)(x-2)\cdots(x-j+1)}{j!}, \quad (x \in \mathbf{R}).$$

关于这些多项式的讨论及我们所需要的一些性质，读者可参阅 § 1.2.

下面假定符号集 Q 是环 $\mathbf{Z}/q\mathbf{Z}$ (这样假定并不失一般性)，对 $\mathbf{x}, \mathbf{y} \in Q^n$，用 $\langle \mathbf{x}, \mathbf{y} \rangle$ 表示通常的内积 $\sum_{i=1}^{n} x_i y_i$.

(5.3.1)引理. 设 ω 是 $\mathbf{C}$ 中的一个 q 次本原单位根，$x \in Q^n$ 是一个固定的重量为 i 的码字，则

$$\sum_{\substack{\mathbf{y} \in Q^n \\ w(\mathbf{y}) = k}} \omega^{\langle \mathbf{x}, \mathbf{y} \rangle} = K_k(i).$$

证明. 我们可以设 $\mathbf{x} = (x_1, x_2, \cdots, x_i, 0, \cdots, 0)$，这里 x_1 到 x_i 都不为 0. 选择 k 个位置 $h_1, h_2, \cdots, h_k$，使得 $0 < h_1 < h_2 < \cdots < h_j \leqslant i < h_{j+1} < \cdots < h_k \leqslant n$，设 D 是所有仅在这些位置上非 0 的字(重为 k) 的集合. 由引理 1.1.32，有

$$\sum_{\mathbf{y} \in D} \omega^{\langle \mathbf{x}, \mathbf{y} \rangle} = \sum_{y_{h_1} \in Q \setminus \{0\}} \cdots \sum_{y_{h_k} \in Q \setminus \{0\}} \omega^{x_{h_1} y_{h_1} + \cdots + x_{h_k} y_{h_k}}$$

$$= (q-1)^{k-j} \prod_{l=1}^{j} \sum_{y \in Q \setminus \{0\}} \omega^{x_{h_l} y} = (-1)^j (q-1)^{k-j},$$

因为D有$\binom{i}{j}\binom{n-i}{k-j}$种选择，所以结论成立。 □

为了能讨论任意码(即不必是线性码)，我们推广(3.5.1)。

(5.3.2)定义． 设 $C \subseteq Q^n$ 是一个含有M个字的码，定义

$$A_i := M^{-1} |\{\langle \mathbf{x}, \mathbf{y} \rangle | \mathbf{x} \in C, \mathbf{y} \in C, d(\mathbf{x}, \mathbf{y}) = i\}|.$$

序列 $(A_i)_{i=0}^n$ 称为C的距离分布或内分布。

注意，如果C是线性的，则距离分布就是重量分布。

下面的引理是线性规划界(定理 5.3.4)的基础。

(5.3.3)引理． 设 $(A_i)_{i=1}^n$ 是码 $C \subseteq Q^n$ 的距离分布，则对于 $k \in \{0, 1, \cdots, n\}$，有

$$\sum_{i=0}^{n} A_i K_k(i) \geqslant 0.$$

证明．由引理 5.3.1，我们有

$$M \sum_{i=0}^{n} A_i K_k(i) = \sum_{i=0}^{n} \sum_{\substack{(\mathbf{x},\mathbf{y}) \in C^2 \\ d(\mathbf{x},\mathbf{y})=i}} \sum_{\substack{\mathbf{z} \in Q^n \\ w(\mathbf{z})=k}} \omega^{\langle \mathbf{x}-\mathbf{y}, \mathbf{z} \rangle}$$

$$= \sum_{\substack{\mathbf{z} \in Q^n \\ w(\mathbf{z})=k}} \left| \sum_{\mathbf{x} \in C} \omega^{\langle \mathbf{x}, \mathbf{z} \rangle} \right|^2 \geqslant 0.$$ □

(5.3.4)定理． 设 $q, n, d \in \mathrm{N}$，$q \geqslant 2$，则

$$A(n, d) \leqslant \max \left\{ \sum_{i=0}^{n} A_i \middle| A_0 = 1,\ A_i = 0,\ 对于\ 1 \leqslant i < d, \right.$$

$$\left. A_i \geqslant 0,\ \sum_{i=0}^{n} A_i K_k(i) \geqslant 0,\ 对于\ k \in \{0, 1, \cdots, n\} \right\}.$$

若 $q = 2$，d 是偶数，则对于奇数i，可取 $A_i = 0$。

证明．由引理 5.3.3，一个 (n, M, d) 码的距离分布满足不等式 $\sum_{i=0}^{n} A_i K_k(i) \geqslant 0$。显然，$A_i$ 是非负的，并且 $A_0 = 1$，$A_i = 0$，

对于 $1\leqslant i<d$. 进一步,由(5.3.2)我们有 $\sum_{i=0}^{n} A_i = M^{-1}|C|^2 = M$.

最后的断言就是问题 4.7.6.

例. 同前面几个例子一样,我们希望估计 $A(13,5)=A(14,6)$,这里 $q=2$. 对于一个 $(14, M, 6)$ 码的距离分布,我们可以假定

$$A_0=1,\ A_1=A_2=A_3=A_4=A_5=A_7$$
$$=A_9=A_{11}=A_{13}=0,$$
$$A_6\geqslant 0,\ A_8\geqslant 0,\ A_{10}\geqslant 0,\ A_{12}\geqslant 0,\ A_{14}\geqslant 0.$$

对于这些 A_i, 由引理 5.3.3, 我们有下述不等式 ($K_k(i)$ 的值可利用(1.2.10)得到):

$$14+2A_6-2A_8-6A_{10}-10A_{12}+14A_{14}\geqslant 0,$$
$$91-5A_6-5A_8-11A_{10}+43A_{12}+91A_{14}\geqslant 0,$$
$$364-12A_6+12A_8+4A_{10}-100A_{12}-364A_{14}\geqslant 0,$$
$$1001+9A_6+9A_8-39A_{10}+121A_{12}+1001A_{14}\geqslant 0,$$
$$2002+30A_6-30A_8+38A_{10}-22A_{12}-2002A_{14}\geqslant 0,$$
$$3003-5A_6-5A_8+27A_{10}-165A_{12}+3003A_{14}\geqslant 0,$$
$$3432-40A_6+40A_8-72A_{10}+264A_{12}-3432A_{14}\geqslant 0.$$

我们必须求出 $M=1+A_6+A_8+A_{10}+A_{12}+A_{14}$ 的一个上界,这个线性规划问题有唯一解:

$$A_6=42,\ A_8=7,\ A_{10}=14,\ A_{12}=A_{14}=0.$$

因此, $M\leqslant 64$. 在 § 4.4 中,我们构造了一个(13, 64, 5)码 Y,于是由此我们证明了 $A(13,5)=64$.

现在,我们给出定理 5.3.4 的另一种形式,与原来的形式相比,它常有一些优点. 熟悉线性规划的读者会看到, 我们应用了对偶原理(参见[32]).

(5.3.5)定理. 设 $\beta(x)=1+\sum_{k=1}^{n}\beta_k K_k(x)$ 是任一多项式, 其中 $\beta_k\geqslant 0\ (1\leqslant k\leqslant n)$, 且满足 $\beta(j)\leqslant 0$, $j=d, d+1, \cdots, n$,

则 $A(n,d)\leqslant\beta(0)$。

证明. 假设 $A_0, A_1, \cdots, A_n$ 满足定理 5.3.4 的条件，即 $K_k(0)+\sum_{i=d}^{n}A_iK_k(i)\geqslant 0\ (k=0,1,\cdots,n;\ A_i\geqslant 0$，对于 $i=d,d+1,\cdots,n)$，则由 β 的条件就可推出 $\sum_{i=d}^{n}A_i\beta(i)\leqslant 0$，即

$$-\sum_{i=d}^{n}A_i\geqslant\sum_{k=1}^{n}\beta_k\sum_{i=d}^{n}A_iK_k(i)$$

$$\geqslant-\sum_{k=1}^{n}\beta_kK_k(0)=1-\beta(0),$$

因此

$$1+\sum_{i=d}^{n}A_i\leqslant\beta(0). \qquad \square$$

定理 5.3.5 的优点是，对于任意满足定理条件的多项式 β 都能产生 $A(n,d)$ 的一个界，而在定理 5.3.4 中，则必须求出不等式组的最优解。

例. 设 $q=2,\ n=2l+1,\ d=l+1$，我们试图求出 $A(n,d)$的一个界. 取 $\beta(x)=1+\beta_1(n-2x)+\beta_2\left(2x^2-2nx+\frac{1}{2}n(n-1)\right)$，选择 β_1 和 β_2 使得 $\beta(d)=\beta(n)=0$，我们有 $\beta_1=(n+1)/2n,\ \beta_2=1/n$，因此定理 5.3.5 的条件满足. 于是，我们得到 $A(2l+1,l+1)\leqslant\beta(0)=1+\beta_1 n+\beta_2\binom{n}{2}=2l+2$. 这与 Plotkin 界(5.2.4)相同.

迄今知道的关于 $\alpha(\delta)$ 的最好的界属于 R. J. McEliece, E. R. Rodemich, H. C. Rumsey 和 L. R. Welch (1977; 参见[50]). 我們不讨论这个界，而只给出一个稍弱的结果 ($\delta>0.273$ 时，实际上是相等的)，这个结果也属于这些作者，它基于定理 5.3.5 的一个应用。

(5.3.6)定理. 设 $q=2$，则

$$\alpha(\delta)\leqslant H_2\left(\frac{1}{2}-\sqrt{\delta(1-\delta)}\right).$$

证明. 我们考虑一个整数 $t\left(1\leqslant t\leqslant\frac{1}{2}n\right)$，和一个在区间 $[0,n]$ 中的实数 a. 定义多项式 $\alpha(x)$ 为

$$\alpha(x):=(a-x)^{-1}\{K_t(a)K_{t+1}(x)-K_{t+1}(a)K_t(x)\}^2.$$

应用(1.2.12)，得

$$(5.3.7)\qquad \alpha(x)=\frac{2}{t+1}\binom{n}{t}\{K_t(a)K_{t+1}(x)-K_{t+1}(a)K_t(x)\}\cdot\sum_{k=0}^{t}\frac{K_k(a)K_k(x)}{\binom{n}{k}}.$$

令 $\alpha(x)=\sum_{k=0}^{2t+1}\alpha_kK_k(x)$ 是 $\alpha(x)$ 的 Krawtchouk 展式，我们希望选取 a 和 t 使得 $\beta(x):=\alpha(x)/\alpha_0$ 满足定理 5.3.5 的条件. 如果我们取 $a\leqslant d$，则仅需检验 $\alpha_i\geqslant 0\ (i=1,\cdots,n)$，$\alpha_0>0$ 是否成立. 若用 $x_1^{(k)}$ 表示 K_k 的最小零点，我们知道 $0<x_1^{(t+1)}<x_1^{(t)}$(见(1.2.13)).

为了简化下面的计算，我们选择 t，使得 $x_1^{(t)}<d$，然后在 $x_1^{(t+1)}$ 和 $x_1^{(t)}$ 之间选择 a 使得 $K_t(a)=-K_{t+1}(a)>0$. 于是，(5.3.7) 把 $\alpha(x)$ 表示为 $\Sigma c_{kl}K_k(x)K_l(x)$，其中所有系数 c_{kl} 都是非负的. 由(1.2.4)可知所有 α_i 也是非负的. 进一步，$\alpha_0=-[2/(t+1)]\binom{n}{t}K_t(a)\cdot K_{t+1}(a)>0$. 因此，确实可以应用定理 5.3.5，从而有

$$(5.3.8)\qquad A(n,d)\leqslant\beta(0)=\frac{\alpha(0)}{\alpha_0}=\frac{(n+1)^2}{2a(t+1)}\binom{n}{t}.$$

为了完成定理的证明，还需要更多地知道零点 $x_1^{(t)}$ 的位置. 我们知道，若 $0<\tau<\frac{1}{2}$，$n\to\infty$ 且 $t/n\to\tau$，则

$$x_1^{(t)}/n \to \frac{1}{2} - \sqrt{\tau(1-\tau)}.$$

由此，可以把(5.3.8)应用于下述情形：$n \to \infty$，$d/n \to \delta$，且有一列 t 值使得 $t/n \to \frac{1}{2} - \sqrt{\delta(1-\delta)}$。在(5.3.8)中取对数，再除以 n，则得定理的结果。（关于 $x_1^{(t)}$ 的命题的证明，建议读者参考一篇有关正交多项式的文献[46]或[53]。） □

§5.4 评　　注

在图2中，我们比较了这章所给出的渐近界，这里没有包括 V. I. Levenshtein（1975；参见[40]）和 V. M. Sidelnikov(1975；参见[63])给出的界，因为它们不如 McEliece 等人的结果[50]好，而且推导相当困难。上面提到的最好界是：

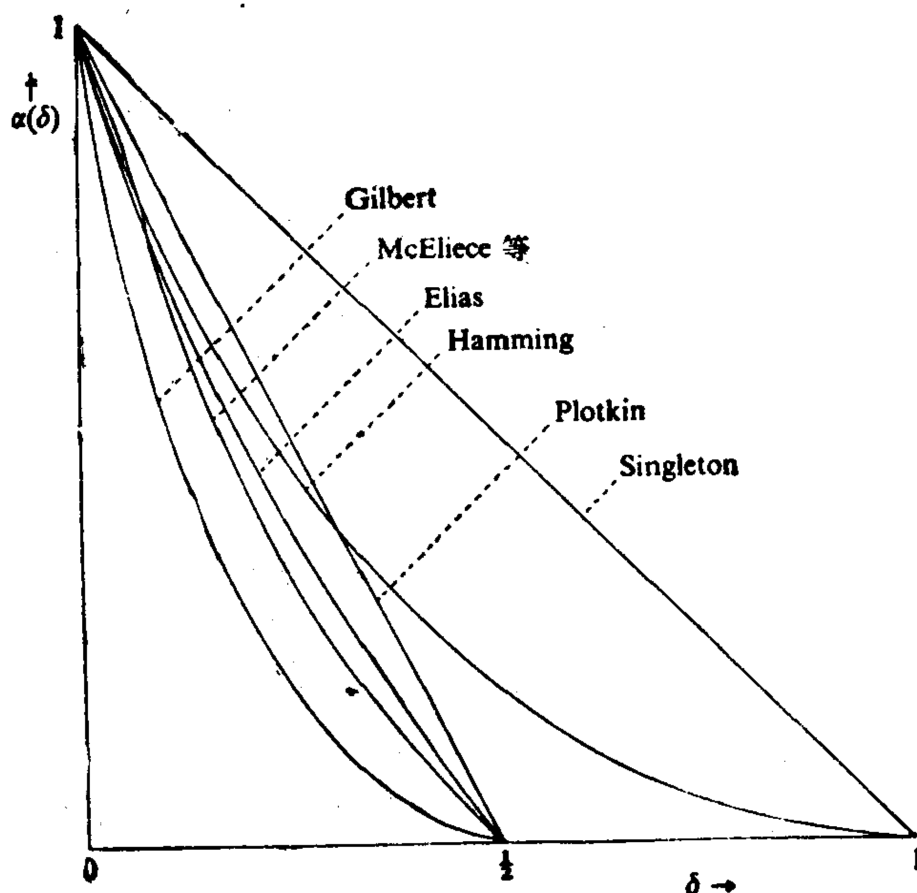


图 2

$$(5.4.1)\quad \alpha(\delta) \leqslant \min\{1 + g(u^2) - g(u^2 + 2\delta u + 2\delta) \mid 0 \leqslant u \leqslant 1 - 2\delta\},$$

其中

$$g(x) := H_2\left(\frac{1-\sqrt{1-X}}{2}\right).$$

其证明可参见[50]或[52].对于很小的值 δ，Elias 界优于(5.3.6)，但劣于(5.4 1)。

M. R. Best 等人(1976；参见[6])对 (5.3.3)，(5.3.4) 作了如下推广：

(i) 如果 $|C|$ 是奇数，则(5.3.3)的不等式要强得多；

(ii) 在(5.3.4)中加上一些不等式(比如明显的不等式 $A_{n-1} + A_n \leqslant 1$)，可以产生几个很好的界(见问题 5.5.12)。

§5.5 问 题

5.5.1. 利用线性码可由它的奇偶校验矩阵定义这样一个事实，证明：如果 $V_q(n-1, d-2) < q^{n-k}$，则存在 $\mathbf{F}_q$ 上的一个 $[n, k, d]$ 码。与定理 5.1.8 比较这一结果。

5.5.2. 对于 $q = 2$，决定 $A(10, 5)$。

5.5.3. 设 $q = 2$，证明：如果定理 5.2.4 的右边是奇整数 l，则 $A(n, d) \leqslant l - 1$。

5.5.4. 若 $q = 2$，决定 $A(17, 8)$ 的界。

5.5.5. 考虑一个[31，5]对偶二元 Hamming 码的生成矩阵。证明可以去掉该矩阵的若干列，使余下的矩阵生成一个 $d = 10$ 的码，达到 Griesmer 界。

5.5.6. 设 C 是一个长为 n、极小距离 $d = 2k$ 的二元码，其码字都具有重量 w。假设 $|C| = [n\cdot(n-1)/w(w-1)]A(n-2, 2k, w-2)$。证明 C 的码字是 2-设计的区组。

5.5 7. 证明缩短二元 Hamming 码是最优的。

5.5.8. 设 $w \in \mathbf{N}$，$w \geqslant 4$，C_l 是如下定义的长为 n 的码：

$$C_l := \left\{(c_0, c_1, \cdots, c_{n-1}) \,\middle|\, \sum_{i=0}^{n-1} c_i = w,\ \sum_{i=0}^{n-1} ic_i \equiv l \pmod{n}\right\},$$

其中求和在 $\mathbf{Z}$ 中进行．证明

$$A(n, 4, w) \sim \frac{n^{w-1}}{w!},\ (n \to \infty).$$

5.5.9. 设 $q = 2$，证明$\binom{n}{w}A(n, 2k) \leqslant 2^n A(n, 2k, w)$.

5.5.10. (i) 证明 $A(n,2k,w) \leqslant (1 - w/k)(1 - (w/n))^{-1}$，如果不等式的右边是一个正数．

(ii) 利用 (i) 和问题 5.5.9 推出 Elias 界．

5.5.11. 设 C 是一个二元 (n, M, d) 码，满足 $n - \sqrt{n} < 2d \leqslant n$．又设 C 有性质：若 $\mathbf{x} \in C$，则 $\mathbf{x} + \mathbf{1} \in C$．证明在(5.3.3)中取 $k = 2$ 可得

$$M \leqslant \frac{8d(n-d)}{n-(n-2d)^2}.$$

(称为 Grey 界.)

5.5.12. 证明 § 4.4 中的(8, 20, 3) 码是最优的．(这是很难的.参见 § 5.4.)

第六章　循　环　码

§6.1　定　　义

在 §4.5 中，我们定义了一个码 C 的自同构群 Aut(C)。与此相应，有一个置换矩阵群．有时，Aut(C) 的定义可以用单项矩阵代替置换矩阵来加以扩充．所谓单项矩阵就是其每个非零元都与一个置换矩阵相对应的矩阵．在这两种情况下，我们感兴趣的都是置换群．这一章将研究这样的线性码，它的自同构群包含几阶循环群，其中 n 是码字长度．

(6.1.1)定义． 一个线性码 C 称为循环码，如果

$$\forall_{(c_0,c_1,\cdots,c_{n-1})\in C}[(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C].$$

用单项矩阵代替置换矩阵，这个定义可扩充如下：如果对于每一个码字 $(c_0,c_1,\cdots,c_{n-1})$，字 $(\lambda c_{n-1},c_0,c_1,\cdots,c_{n-2})$ 也在 C 中(这里 λ 是固定的)，则码叫做常循环码(或负循环码，如果 $\lambda=-1$)．我们将介绍循环码的理论，它到常循环码的推扩是一个简单的练习．

在循环码的讨论中，最重要的工具是 $\mathbf{F}_q^n$ 和一个多项式群之间的下述同构．在多项式环 $\mathbf{F}_q[x]$ 中，x^n-1 的倍式形成 $\mathbf{F}_q[x]$ 的一个理想，剩余类环 $\mathbf{F}_q[x]/(x^n-1)$ 以下列多项式集合为一个代表系，

$$\{a_0+a_1x+\cdots+a_{n-1}x^{n-1}|a_i\in\mathbf{F}_q,\ 0\leqslant i<n\}.$$

很明显，$\mathbf{F}_q^n$ 同构于这个环(仅作为加法群)．下面，我们也要用到现在引进的乘法结构，即模 (x^n-1) 的多项式乘法．从现在起，我们视下述两种表示为同一：

$$(6.1.2)\qquad (a_0,a_1,\cdots,a_{n-1})\in\mathbf{F}_q^n\rightleftarrows(a_0+a_1x+\cdots+a_{n-1}x^{n-1})\in\mathbf{F}_q[x]/(x^n-1).$$

由(6.1.2),谈到码字 **c** 时,我们经常是指码字 $c(x)$. 引伸一步,我们把一个线性码看成是 $\mathbf{F}_q[x]/(x^n-1)$ 的一个子集.

(6.1.3)定理. $\mathbf{F}_q^n$ 中的一个线性码 C 是循环码当且仅当 C 是 $\mathbf{F}_q[x]/(x^n-1)$ 的一个理想.

证明. (i) 如果 C 是 $\mathbf{F}_q[x]/(x^n-1)$ 的一个理想,$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 是任一码字,则,$xc(x)$ 也是 C 中的一个码字,即

$$(c_{n-1}, c_0, c_1, \cdots, c_{n-2})\in C.$$

(ii) 反之,若 C 是循环码,则对每个码字 $c(x)$,都有 $xc(x)$ 在 C 中. 因而,对一切 i, $x^ic(x)$ 在 C 中. 因为 C 是线性的,所以对一切多项式 $a(x)$,都有 $a(x)c(x)\in C$. 因此 C 是一个理想. □

(6.1.4)约定. 从现在起,我们只考虑 $\mathbf{F}_q$ 上长为 n 的循环码,这里 $(n, q)=1$.

由于 $\mathbf{F}_q[x]/(x^n-1)$ 是主理想环,所以,每个循环码 C 由 C 中次数最低的首一多项式 $g(x)$ 的倍式组成(参见 § 1.1).

多项式 $g(x)$ 叫做这个循环码的生成多项式. 它是 x^n-1 的一个因子(若不然,$g(x)$ 与 x^n-1 的最大公因子将是 C 中一个比 $g(x)$ 次数更低的多项式). 令 $x^n-1=f_1(x)f_2(x)\cdots f_t(x)$ 是 x^n-1 的不可约因子分解,由(6.1.4),这些因子互异. 从 x^n-1 的 2^t 个因子中任意取出一个作为生成多项式 $g(x)$,相应地就定义了一个循环码,它是 $g(x) \bmod (x^n-1)$ 的所有倍式的集合. 穷尽全部可能的选取,就得到长为 n 的全部不同的循环码.

(6.1.5)定义. 由 $f_i(x)$ 生成的循环码称为极大循环码(因为它是一个极大理想),记为 M_i^+;由 $(x^n-1)/f_i(x)$ 生成的码称为极小循环码,记为 M_i^-. 极小循环码也称为不可约循环码.

定义(6.1.1)保证了循环码 C 的自同构群包含由置换

$$i\longmapsto i+1 \pmod n$$

生成的循环群. 然而,由于 $a(x^q)=a(x)^q$ 与 $a(x)$ 在同一个循环码中,所以由 $\pi_q(i)=qi \pmod n$ (即 $x\longmapsto x^q$) 定义的置换 π_q 也把循环码映为自身. 若 m 是 $q \pmod n$的阶,则置换 $i\longmapsto i+1$

和 π_q 生成 Aut(C) 的一个 nm 阶子群.

§6.2 生成矩阵和校验多项式

设 $g(x)$ 是一个长为 n 的循环码 C 的生成多项式,如果 $g(x)$ 的次数是 $n-k$, 则码字 $g(x)$, $xg(x)$, $\cdots$, $x^{k-1}g(x)$ 显然构成 C 的一组基,即 C 是一个 $[n, k]$ 码. 因此,若 $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$, 则

$$G = \begin{bmatrix} g_0 & g_1\cdots g_{n-k} & 0 & 0\cdots 0 \\ 0 & g_0\cdots g_{n-k-1} & g_{n-k} & 0\cdots 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & 0 \\ 0 & 0\cdots & g_0 & g_1\cdots g_{n-k} \end{bmatrix}$$

是 C 的生成矩阵. 这意味着我们把信息序列 $(a_0, a_1, \cdots, a_{k-1})$ 编码成 $\mathbf{a}G$, 即多项式

$$(a_0 + a_1x + \cdots + a_{k-1}x^{k-1})g(x).$$

生成矩阵的一个更方便的形式可如下得到: (对于 $i \geqslant k$) 定义 $x^i = g(x)q_i(x) + r_i(x)$, 其中 $r_i(x)$ 是次数小于 $n-k$ 的多项式. 多项式 $x^i - r_i(x)$ 是 C 中的码字,并且构成它的一组基. 由此产生 C 的一个标准形式的生成矩阵 (I_k 在右边). 在这种情况下, $(a_0, a_1, \cdots, a_{k-1})$ 的编码如下: 先用 $g(x)$ 除 $(a_0 + a_1x + \cdots + a_{k-1}x^{k-1})x^{n-k}$, 然后从 $(a_0 + a_1x + \cdots + a_{k-1}x^{k-1})x^{n-k}$ 中减去余式而得到一个码字.

由于用一个固定多项式做除法可由一个简单移位寄存器(定义见第十一章)来实现,所以从技术上说, 这是一个对信息进行编码的十分简单的方法.

因为 $g(x)$ 是 $x^n - 1$ 的因子,所以有多项式 $h(x) = h_0 + h_1x + \cdots + h_kx^k$, 使得 $g(x)h(x) = x^n - 1$ (在 $\mathbf{F}_q[x]$ 中). 在环 $\mathbf{F}_q[x]/(x^n - 1)$ 中, 我们有 $g(x)h(x) = 0$, 即 $g_0h_i + g_1h_{i-1} + \cdots + g_{n-k}h_{i-n+k} = 0$, $i = 0, 1, \cdots, n-1$. 由此即知

$$\begin{bmatrix} 0 & 0\cdots 0 & h_k\cdots h_1 & h_0 \\ 0 & 0\cdots h_k\cdots & h_1 \quad h_0 & 0 \\ \vdots & & & \vdots \\ h_k\cdots\cdots & h_1 & h_0 & 0\cdots 0 \end{bmatrix}$$

是码 C 的奇偶校验矩阵. 我们称 $h(x)$ 为 C 的**校验多项式**. 码 C 由所有使得 $c(x)h(x)=0$ 的 $c(x)$ 组成. 比较矩阵 G 和 H, 我们看到: 以 $h(x)$ 为生成多项式的码等价于 C 的对偶码(颠倒符号次序就可得到). 这个码常常就简单地叫做 C 的对偶码(由于它不等于 $C^{\perp}$,这带来许多混乱). 注意,在这个意义下,极大循环码 M_i^+ 的"对偶"就是极小循环码 M_i^-.

考虑生成多项式为 $g(x)=(x^n-1)/f_i(x)$ 的极小循环码 M_i^-, 其中 $f_i(x)$ 的次数为 k. 如果 $a(x)$ 和 $b(x)$ 是 M_i^- 的两个码字, 并且 $a(x)b(x)=0$, 则其中必有一个能被 $f_i(x)$ 除尽, 因此它就是 0. 因为 M_i^- 没有零因子,所以它是一个域,与 $\mathbf{F}_q^k$ 同构. 一个特别有趣的例子是取 $n=2^k-1$, $f_i(x)$ 为一 k 次本原多项式. 在这种情形下, 生成多项式 $g(x)$ 的 n 个循环移位显然就是 M_i^- 的全部非零码字. 这意味着这个码是等距的(见 § 5.2), 因此它的距离就是 2^{k-1} (由(3.7.5)). 作为推论, 我们得到: x^n-1 的每个本原因子(这里 $n=2^k-1$) 恰好有 2^{k-1} 个系数等于 1.

§ 6.3 循环码的零点

设 $x^n-1=f_1(x)\cdots f_t(x)$, β_i 是 $f_i(x)$ 在 $\mathbf{F}_q$ 的某个扩域中的零点,则 $f_i(x)$ 是 β_i 的极小多项式. 因此,极大码 M_i^+ 无非是满足 $c(\beta_i)=0$ 的多项式 $c(x)$的集合. 所以,一般地可以这样确定一个循环码: 要求它的全部码字都满足某些预先给定的零点. 事实上,我们只需取生成多项式 $g(x)$ 的每个不可约因式 f_i 的一个零点 β_i,并要求所有码字都以这些点为零点(它们在 $\mathbf{F}_q[x]$的某个适当的扩域中). 如果我们从任一集合 $\alpha_1, \alpha_2, \cdots, \alpha_s$ 出发, 定义码 C 为: $c(x)\in C$ 当且仅当 $c(\alpha_i)=0$, $i=1,2,\cdots,s$, 则 C 是

循环的，并且它的生成多项式是 $\alpha_1, \alpha_2, \cdots, \alpha_s$ 的极小多项式的最小公倍．假设所有这些零点都在 $\mathbf{F}_{q^m}$（可表示为向量空间 $\mathbf{F}_q^m$）中．对每个 i，我们考虑以 $1, \alpha_i, \alpha_i^2, \cdots, \alpha_i^{n-1}$ 的向量表示作为列的 $m \times n$ 矩阵，然后将它们放在一起组成一个 $sm \times n$ 矩阵 H，其元素在 $\mathbf{F}_q$ 中．显然，$\mathbf{c}H^T = \mathbf{0}$ 意味着 $c(\alpha_i) = 0$，$i = 1, 2, \cdots, s$，这里 $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1})$．$H$ 的行不一定独立，从中去掉若干行，我们可以得到一个奇偶校验矩阵．作为这种描述循环码的方法的一个例子，我们证明二元（以及许多其它）Hamming 码（参见(3.3.1)）是（等价于）循环码．

(6.3.1)定理．设 $n := (q^m - 1)/(q - 1)$，β 是 $\mathbf{F}_q^m$ 的一个 n 次本原单位根．进一步，令 $(m, q-1) = 1$，则循环码

$$C := \{c(x) \mid c(\beta) = 0\}$$

等价于 $\mathbf{F}_q$ 上的一个 $[n, m-n]$ Hamming 码．

证明．因为

$$n = (q-1)(q^{m-2} + 2q^{m-3} + \cdots + m - 1) + m,$$

我们有 $(n, q-1) = (m, q-1) = 1$．因此 $\beta^{i(q-1)} \neq 1$，即 $\beta^i \notin \mathbf{F}_q$，$i = 1, 2, \cdots, n-1$．由此推出矩阵 H 的列（它们是 $1, \beta, \cdots, \beta^{n-1}$ 在 $\mathbf{F}_q^m$ 中的向量表示形式）在 $\mathbf{F}_q$ 上两两线性独立．故 H 是一个 $[n, n-m]$ Hamming 码的奇偶校验矩阵．

通过构造长为 9 的二元循环码来看看迄今为止我们所学的东西．

(6.3.2)例．包含 9 次本原单位根的 $\mathbf{F}_2$ 的最小扩域是 $\mathbf{F}_{2^6}$．如果 α 是这个域的一个本原元，那么 $\alpha^{63} = 1$，且 $\beta = \alpha^7$ 是一个 9 次本原单位根．由定理 1.1.22，β 的极小多项式以 $\beta, \beta^2, \beta^4, \beta^8, \beta^{16} = \beta^7, \beta^{14} = \beta^5$ 为零点．这个多项式只能是 $(x^9 - 1)/(x^3 - 1) = x^6 + x^3 + 1$（见(1.1.28)）．因此

$$\begin{aligned} x^9 - 1 &= (x-1)(x^2 + x + 1)(x^6 + x^3 + 1) \\ &= f_1(x) f_2(x) f_3(x) \end{aligned}$$

码 M_3^+ 在 H 中的列向量两两独立，即 M_3^+ 的极小距离 $\geqslant 3$．因为 M_3^+ 明显地由下面的码字组成：

$$(c_0\ c_1\ c_2 \quad c_0\ c_1\ c_2 \quad c_0\ c_1\ c_2),$$

所以我们立即得到 $d=3$. 码 M_3^- 的校验多项式为 x^6+x^3+1, 因此它是一个[9, 6]码. 因为 x^3-1 是一个码字,所以距离是 2. 如果我们用 x^6+x+1 来构造 $\mathbf{F}_{2^6}$, 然后用(6.3.1)前面所述的方法对 M_3^- 作一个 12×9 矩阵 H,那么这个矩阵有 6 行是全 0 向量, 一行为全 1 向量, 一行(110 110 110)和四行(011 011 011). 由此,我们找到了一个 3×9 的奇偶校验矩阵. 当然,从 x^6+x^3+1 我们得到一个等价于 (I I I) 的奇偶校验矩阵. 用类似的方法, 读者可给出稍难一些的例子.

§ 6.4 循环码的幂等元

在许多应用中表明了用一个叫做幂等元的多项式 $c(x)$ 代替循环码的生成多项式有其优越性. 幂等元的定义包含在下列定理中.

(6.4.1) 定理. 设 C 是一个循环码, 则 C 中存在唯一的一个码字 $c(x)$ 为其单位元.

证明. 设 $g(x)$是 C 的生成多项式, $h(x)$是 C 的校验多项式, 即 $g(x)h(x)=x^n-1$. 由于 x^n-1 无重零点,有 $(g(x),h(x))=1$.因此存在多项式 $a(x)$和 $b(x)$,使得 $a(x)g(x)+b(x)h(x)=1$. 定义

$$c(x):=a(x)g(x)=1-b(x)h(x).$$

显然, $c(x)$是 C 的一个码字. 而且如果 $p(x)g(x)$ 是 C 的任一码字,那么

$$\begin{aligned} c(x)p(x)g(x) &= p(x)g(x)-b(x)h(x)p(x)g(x) \\ &\equiv p(x)g(x) \bmod (x^n-1). \end{aligned}$$

于是 $c(x)$是 C 的单位元,因此是唯一的. □

因为 $c^2(x)=c(x)$, 所以称 $c(x)$ 为幂等元. 当然, C 中可以有其它元素与其自身的平方相等, 但其中只有一个是码的单位元. 由于每个码字 $v(x)$ 均可写成 $v(x)c(x)$,即 $c(x)$ 的倍式,所

以 $c(x)$生成理想 C.

再一次考虑分解式 $x^n-1=f_1(x)\cdots f_t(x)$. 我们取 $q=2$.由定理 1.1.22 知,这些因子对应于 $\{0, 1,\cdots, n-1\}$ 的分圆陪集分解: $\{0\}$, $\{1, 2, 4,\cdots, 2^r\}$,$\cdots$,$\{a, 2a, \cdots 2^s a\}$, 其中 s 是满足 $a(2^s-1)\equiv 0 \pmod n$ 的最小指数. 在例 6.3.2 中, 这个分解是 $\{0\}$, $\{1, 2, 4, 8, 7, 5\}$ 和 $\{3, 6\}$, 这时 $n=9$. 另一方面, 如果一个幂等元含有项 x^i,则它显然也含有项 x^{2i}. 因此,任一幂等元必是形如 $x^a+x^{2a}+\cdots+x^{2^s a}$ 的幂等元之和, 其中 $\{a, 2a,\cdots, 2^s a\}$ 是某个分圆陪集. 因为恰好有 2^t 个这样的和, 所以我们很容易找到全部可能的幂等元, 从而生成具有给定长度的全部二元循环码. 而根本就不必分解 x^n-1!

我们扩充一点上述理论,还是限定 $q=2$. 首先,从定理 6.4.1 的证明可见,如果 $c(x)$是码 C 的幂等元, $g(x)$ 和 $h(x)$ 分别是 C 的生成多项式和校验多项式,则 $1+c(x)$ 是以 $h(x)$为生成多项式的码的幂等元. 因此, $1+x^n c(x^{-1})$ 是其对偶码的幂等元.

(6.4.2)定义. 不可约循环码 M_i^- 的幂等元叫做*本原幂等元*, 记为 $\theta_i(x)$.

设 α 是在 $\mathbf{F}_2$ 的某个扩域中的一个 n 次本原单位根. 如果多项式 $c(x)$是幂等的,则对所有的 i, $c(\alpha^i)=0$ 或 1. 其逆显然也成立. 如果 $c(x)$ 是一个本原幂等元,则存在 x^n-1 的一个不可约因子 $f(x)$, 使得 $c(\alpha^i)=1$ 当且仅当 $f(\alpha^i)=0$. 即 $c(\alpha^i)=1$ 当且仅当 i 属于某个分圆陪集 $\{a, 2a,\cdots\}$. 这样的本原幂等元常记为 θ_a, 即在(6.4.2)中,指标 i 选自不同分圆陪集的代表系. 例如考虑 $n=15$, 令 α 是 x^4+x+1 的一个零点, 则属于以 x^4+x+1 为校验多项式的极小循环码的本原幂等元记为 θ_1. 在这种情况下, θ_{-1} 对应于非零元 α^{-1}, α^{-2}, α^{-4}, α^{-8}, 即对应于校验多项式 x^4+x^3+1. 在下文中, 如果没有固定这样的 α, 我们就简单地记不可约循环码为 M_1^-, M_2^-,$\cdots$, M_t^-.

(6.4.3)定理. *若 C_1 和 C_2 是分别以 $c_1(x)$ 和 $c_2(x)$ 为幂等元的循环码, 则*

(i) $c_1(x)c_2(x)$ 是 $C_1 \cap C_2$ 的幂等元；

(ii) $c_1(x)+c_2(x)+c_1(x)c_2(x)$ 是 C_1+C_2（即全部码字 $\mathbf{a}+\mathbf{b}$，$\mathbf{a} \in C_1$，$\mathbf{b} \in C_2$）的幂等元.

证明. (i) 是定理 6.4.1 的平凡推论；

(ii) 同理可得. 这是因为 $c_1(x)+c_2(x)+c_1(x)c_2(x)$ 显然在 C_1+C_2 中，而且 C_1+C_2 的码字都有形式 $a(x)c_1(x)+b(x)c_2(x)$. 所以易见 $c_1(x)+c_2(x)+c_1(x)c_2(x)$ 是这个码的幂等元. □

(6.4.4)定理. 对于本原幂等元，我们有

(i) $\theta_i(x)\theta_j(x)=0$，若 $i \neq j$；

(ii) $\sum_{i=1}^{t} \theta_i(x)=1$；

(iii) $1+\theta_{i_1}(x)+\theta_{i_2}(x)+\cdots+\theta_{i_r}(x)$ 是生成多项式为 $f_{i_1}(x)f_{i_2}(x)\cdots f_{i_r}(x)$ 的循环码的幂等元.

证明.

(i) 由定理 6.4.3 得到，因为 $M_i^- \cap M_j^- = \{0\}$；

(ii) 由定理 6.4.3 (ii) 和定理 6.4.4 (i) 得到，因为 $M_1^- + M_2^- + \cdots + M_t^-$ 是全部长为 n 的码字的集合；最后

(iii) 成立，因为 $M_{i_1}^- + \cdots + M_{i_r}^-$ 的校验多项式是 $f_{i_1}(x)\cdots f_{i_r}(x)$.

利用这些定理，寻找本原幂等元并不太困难. 于是，如果生成元是以 $f_{i_1}(x)\cdots f_{i_r}(x)$ 的形式给出的，那么我们有一个确定码的幂等元的简单方法.

在编码理论的几个更深入的课题里，我们会看到涉及幂等元的证明技巧. 本书还达不到这一步. 不过，我们希望再给出一点关于幂等元的结果. 想研究文献的读者将会发现下面的注记是有用的.

考虑一个长为 n、生成元为 $g(x)$ 的循环码 C，设 $x^n-1=g(x)h(x)$. 对两端求形式导数(参见 § 1.1)，我们有

$$x^{n-1}=g'(x)h(x)+g(x)h'(x).$$

这里 $g(x)h'(x)$ 的次数为 $n-1$ 当且仅当 $h(x)$的次数为奇数. 用 x 乘上式两端再关于 x^n-1 取模,得

$$1 = xg'(x)h(x) + xg(x)h'(x) + (x^n - 1),$$

其中, 最后一项消去了另外两个多项式之一中出现的 x^n 这一项. 我们看到C的幂等元是 $xg(x)h'(x) + \delta(x^n - 1)$, 其中, $h(x)$ 为奇数次时 $\delta = 1$;否则 $\delta = 0$. 作为一个例子,考虑长为 15, 校验多项式为 $x^4 + x + 1$ 的极小码,幂等元 θ_1 是 $xg(x) = x(x^{15}-1)/(x^4 + x + 1)$.

下面讨论的关于幂等元之间的对应是一个有用的练习, 我们用上面的例子来加以说明.设 $f(x)$ 是 $x^n - 1$ 的一个本原因子,其中 $n = 2^k - 1$. 再设 α 是 $\mathbf{F}_{2^k}$ 的一个本原元, 满足 $f(\alpha) = 0$. 本原幂等元 θ_1, θ_2 所对应的分圆陪集分别是 $\{1, 2, \cdots, 2^{k-1}\}$ 和 $\{-1, -2, \cdots, -2^{k-1}\}$. 我们断言:

$$\theta_{-1}(x) = \sum_{i=0}^{n-1} \mathrm{Tr}(\alpha^i)x^i,$$

其中 Tr 是迹函数(参见(1.1.29)). 为了证明这一点, 我们必须计算$\theta_{-1}(\alpha^l)$, $l = 0, 1, \cdots, n-1$. 我们有

$$\theta_{-1}(\alpha^l) = \sum_{i=0}^{n-1} (\alpha^l)^i \sum_{j=0}^{k-1} (\alpha^i)^{2^j} = \sum_{j=0}^{k-1} \sum_{i=0}^{n-1} (\alpha^{l+2^j})^i,$$

内部和为 0 ,除非 $\alpha^{l+2^j} = 1$. 因此,若存在 j, 使得 $l = -2^j$, 则 $\theta_{-1}(\alpha^l) = 1$, 否则, $\theta_{-1}(\alpha^l) = 0$. 这证明了结论.

在许多地方都要用到幂等元, 比如计算重量计数子. 我们不打算涉足于这个课题,而是建议读者参看 [42]和 [46]. 本节讨论的内容, 特别是定理 6.4.4, 是半单代数幂等元的一般理论的一个特殊情形. 读者可参阅[16].

§ 6.5 循环码的其它表示

除 § 6.1 介绍的标准方法外, 还有几种其它表示循环码的方法. 使用这些表示法, 有时能使证明更简洁. 我们要讨论的第一

种表示法利用了迹函数(参见(1.1.29)).

(6.5.1)定理. 设 k 是 $p \bmod n$ 的乘法阶, $q=p^k$. 又设 β 是 $\mathbf{F}_q$ 的一个 n 次本原单位根，则集合

$$V:=\{\mathbf{c}(\xi):=(\mathrm{Tr}(\xi), \mathrm{Tr}(\xi\beta), \cdots, \mathrm{Tr}(\xi\beta^{n-1}))\mid \xi\in\mathbf{F}_q\}$$

是 $\mathbf{F}_q$ 上的一个 $[n, k]$ 不可约循环码.

证明. 由定理 1.1.30, V 是一个线性码,又注意到 $\mathbf{c}(\xi\beta^{-1})$ 是 $\mathbf{c}(\xi)$ 的一个循环移位. 因此, V 是循环码. 因为 β 不在 $\mathbf{F}_q$ 的任何真子域中,所以 β 是某个 k 次不可约多项式 $h(x)=h_0+h_1x+\cdots+h_kx^k$ 的零点. 如果 $\mathbf{c}(\xi)=(c_0, c_1, \cdots, c_{n-1})$, 则

$$\sum_{i=0}^{k} c_ih_i=\mathrm{Tr}(\xi h(\beta))=\mathrm{Tr}(0)=0,$$

即,我们得到码 V 的一个奇偶校验方程.

因为 $h(x)$不可约,所以 $x^kh(x^{-1})$ 是 V 的校验多项式,故 V 是一个不可约的 $[n, k]$ 循环码. □

现在我们介绍 Fourier 变换在离散情形的一个模拟. 在编码理论中, 这总是称为 Mattson-Solomon 多项式. 设 β 是 $\mathbf{F}_q$ 的扩域 $\mathscr{F}$ 中的一个 n 次本原单位根. 令 T 是 $\mathscr{F}$ 上次数不超过 $n-1$ 的多项式的集合. 定义 $\Phi: T\to T$ 如下: 设 $a(x)\in T$, 则 $A(X)=(\Phi a)(X)$ 定义为

$$A(X):=\sum_{j=1}^{n} a(\beta^j)X^{n-j}. \tag{6.5.2}$$

若 $\mathbf{a}=(a_0, a_1, \cdots, a_{n-1})$, 则由 $a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ 得到的多项式 $A(X)$ 称为向量 $\mathbf{a}$ 的 Mattson-Solomon 多项式.

(6.5.3)引理. Φ 的逆由下式给出:

$$a(x)=n^{-1}(\Phi A)(x^{-1}) \pmod{x^n-1}.$$

证明.

$$A(\beta^k)=\sum_{j=1}^{n}\sum_{i=0}^{n-1} a_i\beta^{ij}\beta^{-kj}=\sum_{i=0}^{n-1} a_i\sum_{j=0}^{n}\beta^{(i-k)j}=na_k. \quad \square$$

用 $\circ$ 表示多项式 $\bmod(x^n-1)$ 的乘法,设$*$ 定义为

$$(\sum a_ix^i)*(\sum b_ix^i)=\sum a_ib_ix^i,$$

则易见Φ是环$(T,+,\circ)$到$(T,+,*)$上的一个同构.

现在,我们利用这些多项式研究循环码.

(6.5.4)引理. 设V是由

$$g(x)=\prod_{k\in K}(x-\beta^k)$$

生成的$\mathbf{F}_q$上的循环码. 假设$\{1,2,\cdots,d-1\}\subset K$, $\mathbf{a}\in V$, 则$\mathbf{a}$的Mattson-Solomon多项式A的次数至多为$n-d$.

证明. 因为$a(x)$可被$g(x)$整除,所以对于$1\leqslant j\leqslant d-1$, $a(\beta^j)=0$. 结论由(6.5.2)推出. □

(6.5.5)定理. 若字$\mathbf{a}$的Mattson-Solomon多项式A的零点中有r个n次单位根,则$w(\mathbf{a})=n-r$.

证明. 这是引理6.5.3的直接推论. □

我们也可以建立循环码与线性递推序列之间的联系,关于线性递推序列有大量的文献(例如见[61]). 一个元素在$\mathbf{F}_q$中的线性递推序列是由初始序列$a_0, a_1,\cdots,a_{k-1}$及递推关系

$$a_l+\sum_{i=1}^{k}b_ia_{l-i}=0\,(l\geqslant k) \tag{6.5.6}$$

定义的.

求解(6.5.6)的标准方法是试验$a_l=\beta^l$. 它是(6.5.6)的一个解,如果β是$h(x)$的零点,其中

$$h(x):=x^k+\sum_{i=1}^{k}b_ix^{k-i}.$$

我们假定方程$h(x)=0$在$\mathbf{F}_q$的某个扩域中有k个互异零点$\beta_1,\beta_2,\cdots,\beta_k$. 于是,对任意的$c_1,c_2,\cdots,c_k$, 序列

$$a_l=\sum_{i=1}^{k}c_i\beta_i^l$$

都是(6.5.6)的解. 我们必须选择c_i以使$a_1,a_2,\cdots,a_k$取预先给定的值. 这相当于解k个联立线性方程,其系数行列式是一个Vandermonde行列式

$$
(6.5.7)\quad \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_k \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_k^2 \\ \cdots & \cdots & \cdots & \cdots \\ \beta_1^{k-1} & \beta_2^{k-1} & \cdots & \beta_k^{k-1} \end{vmatrix} = \prod_{i>j} (\beta_i - \beta_j) \neq 0.
$$

因此，我们的确可以找到所求序列.

假设 $h(x)$是 $x^n - 1$ 的一个因式(仍设 $(n, q) = 1$)，则线性递推序列是周期的，周期是 n 的一个因子. 现在考虑所有的部分序列 $(a_0, a_1, \cdots, a_{n-1})$，其中 $(a_0, a_1, \cdots, a_{k-1})$ 跑遍 $\mathbf{F}_q^k$，则我们有一个 $[n, k]$ 循环码，它以 $x^k h(x^{-1})$ 为校验多项式. 因此，

$$
C = \left\{ (a_0, \cdots, a_{n-1}) \mid a_l = \sum_{i=1}^{k} c_i \beta_i^l \ (0 \leqslant l < n), \right.
$$

$$
\left. \times (c_1, c_2, \cdots, c_k) \in \mathbf{F}_q^k \right\}
$$

是循环码的另一种表示.

§ 6.6 BCH 码

在实际中还在大量使用的一类重要的循环码，是由 R.C. Bose 和 D. K. Ray-Chaudhuri 以及 A. Hocquenghem (独立地) 发现的，这类码就是 BCH 码.

(6.6.1)定义. $\mathbf{F}_q$ 上长为 n 的循环码称为一个设计距离为 δ 的 BCH 码，如果它的生成元 $g(x)$是 $\beta^l, \beta^{l+1}, \cdots, \beta^{l+\delta-2}$ 的极小多项式的最小公倍. 这里，l 是某个整数，β 是一个 n 次本原单位根. 通常，我们取 $l = 1$ (有时称之为狭义 BCH 码). 若 $n = q^m - 1$，即 β 是 $\mathbf{F}_{q^m}$ 的一个本原元，则称这个 BCH 码是本原的.

下述定理解释了"设计距离"这一术语.

(6.6.2)定理. 一个设计距离为 δ 的 BCH 码的极小距离至少是 δ.

证明一. 用与 § 6.3 相同的方法，我们作一个 $m(d-1) \times n$ 矩阵 H:

$$H:=\begin{bmatrix} 1 & \beta^{l} & \beta^{2l} & \cdots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \cdots & \beta^{(n-1)(l+1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \beta^{l+d-2} & \beta^{2(l+d-2)} & \cdots & \beta^{(n-1)(l+d-2)} \end{bmatrix}$$

其中每个元素都看作 $\mathbf{F}_q$ 上的长为 m 的向量. 一个字 $\mathbf{c}$ 在 BCH 码中当且仅当 $\mathbf{c}H^T=\mathbf{0}$. H 的 $m(d-1)$ 个行不一定线性独立. 考虑 H 的任意 $d-1$ 列, 令 $\beta^{i_1 l},\cdots,\beta^{i_{d-1}l}$ 是这些列顶端的元素. 这样得到的 H 的子矩阵的行列式是一个 Vandermonde 行列式(参看(6.5.7)). 因为 β 是一个 n 次本原单位根, 所以这个行列式的值为 $\beta^{(i_1+\cdots+i_{d-1})l}\prod_{r>s}(\beta^{i_r}-\beta^{i_s})\neq 0$. 因此, H 的任意 $d-1$ 列都是线性独立的. 于是, 码字 $\mathbf{c}\neq\mathbf{0}$ 的重量 $\geqslant d$.

证明二. 不失一般性, 取 $l=1$. 由引理 6.5.4, 码字 $\mathbf{c}$ 的 Mattson-Solomon 多项式的次数至多是 $n-d$, 因此在定理 6.5.5 中有 $r\leqslant n-d$, 即 $w(\mathbf{c})\geqslant d$. □

注. 定理 6.6.2 通常称为 BCH 界. 从现在起我们一般只考虑狭义 BCH 码. 如果我们从 $l=0$ 而不是从 $l=1$ 出发, 则得到狭义码的偶重量子码.

例. 设 $n=31$, $m=5$, $q=2$, $d=8$. 令 α 是 $\mathbf{F}_{2^5}$ 的一个本原元, 其极小多项式为

$$(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16}).$$

用同样的方法可得 $m_3(x)$. 但

$$\begin{aligned} m_5(x) &= (x-\alpha^5)(x-\alpha^{10})(x-\alpha^{20})(x-\alpha^9)(x-\alpha^{18}) \\ &= m_9(x). \end{aligned}$$

这表明 $g(x)$ 是 $m_1(x)$, $m_3(x)$, $m_5(x)$, $m_7(x)$, $m_9(x)$ 的最小公倍. 因此, 设计距离是 8 (显然至少是 9) 的本原 BCH 码的极小距离实际上至少是 11.

下面的定理属于 C.R.P. Hartmann 和 K.K. Tzeng (1972; 见[33]), 它是 BCH 界的一个推广. 这里的证明是 C. Roos 新近给出的(未发表).

(6.6.3)定理. 设C是$\mathbf{F}_q$上以$g(x)$为生成元的一个长为n的循环码，β是$\mathbf{F}_{q^m}$的一个n次本原单位根．若$(n, c_1)=1$，$(n, c_2)<d_0$，且$g(\beta^{l+i_1c_1+i_2c_2})=0\ (i_1=0,1,\cdots,d_0-2; i_2=0,1,\cdots,s)$，则$C$的极小距离$d$满足$d\geqslant d_0+s$.

证明.

(i) 设$A=[\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_n]$是域$K$上的矩阵，使得任意$k-1$列都线性无关．又设$x_1, x_2, \cdots, x_n$是$K$中的一列元素，且$K$中任一元素在其中至多出现$k-1$次．于是在矩阵

$$A'=\begin{bmatrix}\mathbf{a}_1, & \mathbf{a}_2, & \cdots, & a_n\\ x_1\mathbf{a}_1, & x_2\mathbf{a}_2, & \cdots & x_n\mathbf{a}_n\end{bmatrix}$$

中任意k列都线性无关．为了证明这一点，假设A'含有k个线性无关的列，不失一般性，就设为前k列．因而存在不全为0的元素$\lambda_1, \cdots, \lambda_k\in K$，使得

$$\sum_{i=1}^{k}\lambda_i\mathbf{a}_i=\sum_{i=1}^{k}\lambda_ix_i\mathbf{a}_i=\mathbf{0}.$$

于是

$$\sum_{i=1}^{k-1}\lambda_i(x_i-x_k)\mathbf{a}_i=\mathbf{0}.$$

由于A的任意$k-1$列都线性独立，这意味着$\lambda_i(x_i-x_k)=0$，$1\leqslant i\leqslant k-1$．但$\lambda_i\neq 0$，$1\leqslant i\leqslant k$，这亦由$A$的任意$k-1$列都线性无关这一事实得到．因此，$x_1=x_2=\cdots=x_k=0$．矛盾.

(ii) 令$N=\{\alpha_1, \alpha_2, \cdots, \alpha_t\}$是$\mathbf{F}_{q^m}$中$n$次单位根的一个非空集合．$H_N$是以$(1, \alpha_i, \cdots, \alpha_i^{n-1})(1\leqslant i\leqslant t)$为行的一个$t\times n$矩阵．$H_N$是$\mathbf{F}_q$上一个循环码$C_N$的奇偶校验矩阵，$C_N$的极小距离为$d$．我们也可把$H_N$看成$\mathbf{F}_{q^m}$上一个码$C_N^*$的奇偶校验矩阵．如果$C_N^*$的极小距离为$d^*$，则显然有$d\geqslant d^*$．现在，设$\alpha$是一个阶为$e>n/d^*$的$n$次单位根，则在序列$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$中每个元素出现$n/e<d^*$次．因此，作为(i)的直接推论，以$H_{N\cup\alpha N}$为奇偶校验矩阵的码的极小距离$\geqslant d^*+1$.

(iii) 设 C^* 是 $\mathbf{F}_{q^m}$ 上的一个以 $g(x)$为生成元的循环码,极小距离为 d^*. 我们证明 $d^* \geqslant d_0 + s$, 因为 $d \geqslant d^*$, 这就推出了定理. 对于 $s = 0$, 结论由定理 6.6.2 推出(定理 6.6.2 也可用(ii)和对 δ 作归纳法得到).

设 $s \geqslant 0$, 并假定定理成立,即

$$N = \{\beta^{l+i_1c_1+i_2c_2} | 0 \leqslant i_1 \leqslant d_0 - 2,\ 0 \leqslant i_2 \leqslant s\}$$

定义了一个满足 $d^* \geqslant d_0 + s$ 的码. 令 $\alpha = \beta^{c_2}$,则α的阶 $e = n/(n, c_2) > n/d_0 \geqslant n/d^*$. 如果我们应用 (ii), 则定理结论对 $s+1$ 也为真. □

例. 设 $n = 51$, $g(x) = m_1(x)m_9(x)$. $g(x)$ 的零点是 β^i,其中 $i = 1, 2, 4, 8, 16, 32, 13, 26$ 和 $9, 18, 36, 21, 42, 33, 15, 30$. 码是 35 维的. 由 BCH 界知 $d \geqslant 3$. 但考虑到 $l = 1, c_1 = 1$, $c_2 = 7$ 对应于 $i = 1, 2, 8, 9, 15, 16$, 由定理 6.6.3 推得 $d \geqslant 5$.

一般地,找出 BCH 码确切的极小距离是个难题. 然而,这里也有可谈的工作. 为了阐明这一点,我们限定讨论二元本原 BCH 码. 首先,必须证明一个引理. 视 $\mathbf{F}_{2^k}$ 为空间 $\mathbf{F}_2^k$,设U是一个l-维子空间,定义 $\sum_i (U) = \sum_{x \in U} x^i$.

(6.6.4)引理. *若 i 的二进制表达式中 1 的个数小于l,则*

$$\sum_i (U) = 0.$$

证明. 我们用归纳法. $l = 1$ 的情形是平凡的. 假设结论对某个 l 为真, 令V是 $l+1$ 维的且 $V = U \cup (U + b)$, 其中U的维数是l,则

$$\sum_i (V) = \sum_i (U) + \sum_{x \in U} (x + b)^i + \sum_{\nu=0}^{i-1} \binom{i}{\nu} b^{i-\nu} \sum_\nu (U).$$

如果 i 的二元展开式中至多有 l 个 1, 则由定理 4.5.1, 二次系数 $\binom{i}{\nu} = 0$, $\nu < i$, 除非ν的二元展开式中 1 的个数小于 l. 而这时由归纳法假设亦得

$$\sum_{v}(U)=0. \qquad \square$$

(6.5.5)定理. 字长为 $n=2^m-1$，设计距离为 $\delta=2^l-1$ 的本原的二元 BCH 码的极小距离为 δ.

证明. 设 U 是 $\mathbf{F}_{2^m}$ 的一个 l-维子空间. 考虑向量 $\mathbf{c}$,它恰在相应于 U 的非零元素的位置上为 1, 即

$$c(x)=\sum_{i:\alpha^i\in U\backslash\{0\}}x^i.$$

令 $1\leqslant i<2^l-1$, 则 i 的二元展开式中 1 的个数小于 l. 进一步, $c(\alpha^i)=\sum_{i}(U)$, 因此,由引理 6.6.4 我们有 $c(\alpha^i)=0$, $1\leqslant i\leqslant 2^l-1$. 即 $C(x)$ 是 C 的一个码字. $\square$

(6.6.6)推论. 一个设计距离为 δ 的本原 BCH 码的极小距离 $d\leqslant 2\delta-1$.

证明. 在定理 6.6.5 中取 l 使得 $2^{l-1}\leqslant\delta\leqslant 2^l-1$, 则定理 6.6.5 中的码是这个设计距离为 δ 的码的子码.

对于 BCH 码的确切维数给出一个适当的估计虽然并不极端困难,但会占去太大篇幅. 在二元情形, 如果 $\nu=2t+1$, 我们有估计 2^m-1-mt. 对于大的 t,显然这是很差的,尽管对于(与 m 比较)小的 t 它是精确的. 建议有兴趣的读者参阅 [46]. 结合这些估计,我们容易证明,长的本原 BCH 码在第五章的意义是坏的,即如果 C_ν 是一个本原 $[n_\nu, k_\nu, d_\nu]$ BCH 码,其中 $\nu=1,2,\cdots$,和 $n_\nu\to\infty$, 则 $k_\nu/n_\nu\to 0$ 或 $d_\nu/n_\nu\to 0$.

在 § 6.1 中我们已经指出, $\mathbf{F}_q$ 上长为 n 的循环码的自同构群不仅包含循环置换,也包含 π_q. 对于 BCH 码,我们能证明更多的东西. 考虑 $\mathbf{F}_q$ 上一个本原 BCH 码 C,其长为 $n=q^m-1$,设计距离为 d (即 $\alpha,\alpha^2,\cdots,\alpha^{d-1}$ 是码字的预先给定的零点, 其中 α 是 $\mathbf{F}_{q^m}$ 的一个本原元).

我们用 $X_i=\alpha^i$ $(i=0,1,\cdots,n-1)$ 记码字中符号的位置. 加上奇偶校验位,我们把码扩充为 $\bar{C}$. 附加的位置用∞记之,

关于∞的运算我们作显然的约定．码字（$c_0, c_1, \cdots, c_\infty$）表示为 $c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + c_\infty x^\infty$．进一步约定：$1^\infty := 1$，$(\alpha^i)^\infty = 0$，对 $i \not\equiv 0 \pmod n$．

现在我们证明 $\bar{C}$ 在仿射置换群 AGL$(1, q^m)$ 对位置的作用下保持不变(参见 § 1.1)． 这个群由下列置换组成

$$P_{u,v}(X) := uX + v, \ (u \in \mathbf{F}_{q^m}, v \in \mathbf{F}_{q^m}, u \neq 0).$$

这是一个 2-传递群．首先注意到 $P_{\alpha,0}$ 是在 C 的位置上的一个循环移位，且保持∞不动．设 $(c_0, c_1, \cdots, c_{n-1}, c_\infty) \in C$，经 $P_{u,v}$ 置换得到的字记为 $(c'_0c'_1, \cdots, c'_{n-1}, c'_\infty)$，则对于 $0 \leqslant k \leqslant d-1$，我们有

$$\sum_i c'_i \alpha^{ik} = \sum_i c_i(u\alpha^i + v)^k = \sum_i c_i \sum_{l=0}^{k} \binom{k}{l} u^l \alpha^{il} v^{k-l}$$

$$= \sum_{l=0}^{k} \binom{k}{l} u^l v^{k-l} \sum_i c_i (\alpha^l)^i = 0.$$

这是因为由 $\mathbf{c} \in C$ 推知对于 $0 \leqslant l \leqslant d-1$，内和为 0．故有下述定理．

(6.6.7)定理．长为 $n+1 = q^m$ 的每个扩充本原 BCH 码都以 AGL$(1, q^m)$ 为一自同构群．

(6.6.8)推论． 2 元本原 BCH 码的极小距离为奇数．

证明．设 C 是一个这样的码，我们已经证明了 Aut $(\bar{C})$ 关于位置是传递的．如果我们只考虑 $\bar{C}$ 中重量最小的码字，那么这也为真． 于是 $\bar{C}$ 中存在一个在最后那个校验位为 1 的最小重量码字． □

§ 6.7 BCH 码的译码

我们继续考虑 $\mathbf{F}_q$ 上的长为 n，设计距离为 $\delta = 2t+1$ 的 BCH 码，并设 β 是 $\mathbf{F}_{q^m}$ 的一个 n 次本原单位根． 考虑一个码字 $C(x)$，其接收字设为

$$R(x) = R_0 + R_1x + \cdots + R_{n-1}x^{n-1}.$$

令 $E(x):=R(x)-C(x)=E_0+E_1x+\cdots+E_{n-1}x^{n-1}$ 表示差错向量．定义

$M:=\{i|E_i\neq 0\}$，出现差错的位置；

$e:=|M|$，差错个数；

$\sigma(z):=\prod_{i\in M}(1-\beta^i z)$，称之为**差错位置多项式**；

$$\omega(z):=\sum_{i\in M}E_i\beta^i z\prod_{j\in M\setminus\{i\}}(1-\beta^j z).$$

显然，如果我们能求出多项式 $\sigma(z)$ 和 $\omega(z)$，那么即能纠正差错，事实上，一个差错发生在位置 i 当且仅当 $\sigma(\beta^{-i})=0$．此时，差错就是 $E_i=-\omega(\beta^{-i})\beta^i/\sigma'(\beta^{-i})$．从现在起我们假定 $e\leqslant t$（若 $e>t$，是不能指望纠正这些差错的）．注意到

$$\frac{\omega(z)}{\sigma(z)}=\sum_{i\in M}\frac{E_i\beta^i z}{1-\beta^i z}=\sum_{i\in M}E_i\sum_{l=1}^{\infty}(\beta^i z)^l$$

$$=\sum_{l=1}^{\infty}z^l\sum_{i\in M}E_i\beta^{li}=\sum_{l=1}^{\infty}z^l E(\beta^l),$$

其中所有的运算都是利用 $\mathbf{F}_{q^m}$ 上的形式幂级数进行的．对于 $1\leqslant l\leqslant 2t$，我们有 $E(\beta^l)=R(\beta^l)$，即接收者知道等式右边的前 $2t$ 个系数．因此，$\omega(z)/\sigma(z)\bmod z^{2t+1}$ 就是已知的．我们断言，接收者必须决定多项式 $\sigma(z)$ 和 $\omega(z)$，使得 $\deg\omega(z)\leqslant\deg\sigma(z)$，并在下述条件

$$\frac{\omega(z)}{\sigma(z)}\equiv\sum_{l=1}^{2t}z^l R(\beta^l)\pmod{z^{2t+1}}$$

之下使 $\deg\sigma(z)$ 尽可能地小．令 $S_l:=R(\beta^l)$，$l=1,\cdots,2t$；又令 $\sigma(z)=\sum_{i=0}^{e}\sigma_i z^i$，则

$$\omega(z)\equiv\left(\sum_{l=1}^{2t}S_l z^l\right)\left(\sum_{i=0}^{e}\sigma_i z^i\right)$$

$$=\sum_k z^k\left(\sum_{i+l=k}S_l\sigma_i\right)\pmod{z^{2t+1}}.$$

因为 $\omega(z)$ 的次数 $\leqslant e$，所以

$$\sum_{i+l=k} S_l\sigma_i = 0, \quad \text{当} \ e+1 \leqslant k \leqslant 2t.$$

这是一个以 $\sigma_1, \cdots, \sigma_e$ 为未定元的线性方程组，含有 $2t-e$ 个线性方程(已知 $\sigma_0=1$). 设 $\tilde{\sigma}(z)=\sum_{i=0}^{e}\tilde{\sigma}_i z^i$ (其中 $\tilde{\sigma}_0=1$)是方程组的解中次数最低的多项式(已知至少存在一个解 $\sigma(z)$). 对于 $e+1\leqslant k\leqslant 2t$，我们有

$$0=\sum_{l} S_{k-l}\tilde{\sigma}_l=\sum_{i\in M}\sum_{l} E_i\beta^{(k-l)i}\tilde{\sigma}_e$$

$$=\sum_{i\in M} E_i\beta^{ik}\tilde{\sigma}(\beta^{-i}).$$

可以视右边为一个以 $E_i\tilde{\sigma}(\beta^{-i})$ 为未定元、β^{ik} 为系数的线性方程组，因此它的系数行列式也是一个 Vandermonde 行列式，所以 $\neq 0$. 于是，对于 $i\in M$，$E_i\tilde{\sigma}(\beta^{-i})=0$. 因为 $E_i\neq 0$，$i\in M$，我们看到 $\sigma(z)$ 整除 $\tilde{\sigma}(z)$，即 $\tilde{\sigma}(z)=\tilde{\sigma}(z)$. 因此，次数最低的解 $\tilde{\sigma}(z)$的确解决了我们的问题. 而且我们已经看到求 $\tilde{\sigma}(z)$ 相当于解一个线性方程组. 这个方法的优点是译码者有一个不依赖于 e 的算法. 当然，在实际应用中，找一个快速算法来实现我们仅从理论上考虑的这个问题更为重要. 这样的算法(及其实现)已由 Berlekamp(参见[2],[24])设计出来，通常称之为 Berlekamp 译码器.

§ 6.8 Reed-Solomon 码

BCH 码的一个最简单的实例，即 $n=q-1$ 的情形有许多重要的应用.

(6.8.1)定义. 一个 Reed-Solomon 码 (RS 码)是 $\mathbf{F}_q$ 上长为 $n=q-1$ 的本原 BCH 码. 这种码的生成元具有形式 $g(x)=\prod_{i=1}^{d-1}(x-\alpha^i)$，其中 α 是 $\mathbf{F}_q$ 的一个本原元.

由 BCH 界(6.6.2),以上述 $g(x)$ 为生成元的 RS 码的极小距离至少是 d. 由 § 6.2, 这个码是 $k=n-d+1$ 维的. 因此, 推论 5.2.2 蕴含其极小距离是 d. 故, RS 码是极大距离可分码.

假设我们需要一个码用于这样一个信道, 它的错误并不是随机产生的(如 B.S.C), 而是突发的(即几个错误靠在一起). 在实际应用中这是经常遇到的(如电信、磁带). 对于这样的信道,常常是使用RS 码. 我们对它作一简要说明. 假设二元信息取成一列 m 个符号, 视之为 $\mathbf{F}_{2^m}$ 的元素. 如果以 RS 码来编这些信息, 则含几个差错的一个突出错误只影响 RS 码中一个码字的几个相继符号. 自然, 这个想法可用于任何码. 但由于 RS 码是极大距离可分码,因而它就显得特别有用. 一个更重要的应用将在 § 9.2 中讨论. 与此应用相联系,我们提一下 Reed 和 Solomon 的原始方法. 设 $n=q-1$, α 是 $\mathbf{F}_q$ 的一个本原元. 象通常一样,把 $\mathbf{a}=(a_0, a_1, \cdots, a_{k-1})\in\mathbf{F}_q^k$ 和 $a_0+a_1x+\cdots+a_{k-1}x^{k-1}$ 等同起来, 则

$$C=\{(c_0, c_1, \cdots, c_{n-1})\mid c_i=a(\alpha^i), 0\leqslant i<n, \mathbf{a}\in\mathbf{F}_q^k\}$$

是一个 RS 码,且 $d=n-k+1$. 要弄清这点, 首先注意 C 是循环的. C 的定义和引理 6.5.3 蕴含码字 $\mathbf{c}$ 的 Mattson-Solomon 多项式为 $na(x)$. 因为 $a(x)$的次数 $\leqslant k-1$,则 $c(\alpha^i)=0$, $i=1, 2, \cdots, n-k$. 因此, C 是 RS 码. 这个表示虽然不是系统的, 但却给出了 RS 码的一个非常有效的编码算法.

§ 6.9 二次剩余码

在这一节中,我们要考虑字长 n 为奇素数的码. 字母表 $\mathbf{F}_q$ 必须满足条件: q 是一个模 n 的二次剩余,即 $q^{(n-1)/2}\equiv 1 \pmod n$. 象通常一样, α 表示 $\mathbf{F}_q$ 的某个扩域中的一个 n 次本原单位根. 以后会发现我们还要求 α 满足另一个条件. 我们定义

$R_0:=\{i^2 \pmod n)\mid i\in\mathbf{F}_n, i\neq 0\}$, $\mathbf{F}_n$ 中的二次剩余,

$R_1:=\mathbf{F}_n^*\backslash R_0$, $\mathbf{F}_n$ 中的非二次剩余,

$$g_0(x):=\prod_{r\in R_0}(x-\alpha^r),\quad g_1(x):=\prod_{r\in R_1}(x-\alpha^r).$$

因为我们已经要求 $q(\bmod n)$ 在 R_0 中,所以多项式 $g_0(x)$ 和 $g_1(x)$ 的系数都在 $\mathbf{F}_q$ 中(参见定理 1.1.22). 更进一步,

$$x^n-1=(x-1)g_0(x)g_1(x).$$

(6.9.1)定义. $\mathbf{F}_q$ 上长为 n,生成元为 $g_0(x)$ 或 $(x-1)$. $g_0(x)$ 的循环码叫做*二次剩余码* (QR 码).

我们只考虑二元情形的扩充 QR 码,定义同 (3.2.7). 这个码可由 $g_0(x)$ 生成的码加上奇偶校验位得到.

对于其它的域, 我们通常修改扩充码的定义, 使得 $n\equiv-1(\bmod 4)$ 时扩充码是自对偶的, $n\equiv1(\bmod 4)$ 时,对偶于以 $g_1(x)$ 为生成元的码的扩充码(参见[46]). 在二元情形,生成元为 $(x-1)g_0(x)$ 的码是另一个 QR 码的偶重量子码. 如果 G 是前者的生成矩阵, 则在 G 上加一全 1 行即得后者的生成矩阵. 如果先在 G 上加一全 0 列,然后再加一全 1 行,那么得到的是扩充码的生成矩阵.

在二元情形, q 是模 n 二次剩余意味着 $n\equiv\pm1(\bmod 8)$ (参见 § 1.1). 作用于码字位置上的置换 $\pi_j:i\longmapsto ij\ (\bmod n)$, 将以 $g_0(x)$ 为生成元的码映到自身(若 $j\in R_0$) 或映到以 $g_1(x)$ 为生成元的码(若 $j\in R_1$). 因此,以 $g_0(x)$ 为生成元的码等价于以 $g_1(x)$ 为生成元的码. 若 $n\equiv-1(\bmod 4)$, 则 $-1\in R_1$, 在这种情形, 变换 $x\to x^{-1}$ 把以 $g_0(x)$ 为生成元的码的码字映为以 $g_1(x)$ 为生成元的码的码字.

(6.9.2)定理. *如果* $\mathbf{c}=c(x)$ *是生成元为* $g_0(x)$ *的* QR *码的码字, 且* $c(1)\neq0$, $w(\mathbf{c})=d$, *那么*

(i) $d^2\geqslant n$,

(ii) *若* $n\equiv-1\ (\bmod 4)$, *则* $d^2-d+1\geqslant n$,

(iii) *若* $n\equiv-1(\bmod 8)$, $q=2$, *则* $d\equiv3(\bmod 4)$.

证明

(i) 因为 $c(1)\neq0$, 所以多项式 $c(x)$ 不能被 $(x-1)$ 整除.

通过适当的置换 π_j，我们可以将 $c(x)$ 变成能被 $g_1(x)$ 整除的多项式 $\hat{c}(x)$，当然，$\hat{c}(x)$ 也不被 $(x-1)$ 整除. 这意味着 $c(x)\hat{c}(x)$ 是 $1+x+x^2+\cdots+x^{n-1}$ 的倍式. 因为多项式 $c(x)\hat{c}(x)$ 至多有 d^2 个非零系数，所以我们证明了第一个结论.

(ii) 在上面的证明中，取 $j=-1$，这时显然 $c(x)\hat{c}(x)$ 至多有 d^2-d+1 个非 0 系数.

(iii) 设 $c(x)=\sum_{i=1}^{d} x^{l_i}$，$\hat{c}(x)=\sum_{i=1}^{d} x^{-l_i}$. 如果 $l_i-l_j=l_k-l_l$，则 $l_j-l_i=l_l-l_k$. 因此，若积 $c(x)\hat{c}(x)$ 中的某项消去，一次就消去了 4 项. 所以对于某个 $a\geqslant 0$，$n=d^2-d+1-4a$.

□

§ 6.4 中介绍了循环码的幂等元，它对于 QR 码的分析是一个强有力的工具.

(6.9.3)定理. 对于 $\mathbf{F}_q$ 的一个适当选择的本原元 α，多项式

$$\theta(x):=\sum_{r\in R_0} x^r$$

是一个 QR 码的幂等元. 当 $n\equiv 1 \pmod 8$ 时，这个 QR 码的生成元为 $(x-1)g_0(x)$，当 $n\equiv -1 \pmod 8$ 时，生成元为 $g_0(x)$.

证明. $\theta(x)$ 显然是一个幂等多项式，因此 $\{\theta(\alpha)\}^2=\theta(\alpha)$，即 $\theta(\alpha)=0$ 或 1. 同理，若 $i\in R_0$，则 $\theta(\alpha^i)=\theta(\alpha)$；若 $i\in R_1$，则 $\theta(\alpha^i)+\theta(\alpha)=1$. α 的“适当选择”在于使 $\theta(x)=0$（读者可以自己证明 $\mathbf{F}_q$ 上的全部本原元都满足 $\theta(\alpha)=1$ 是不可能的）. 我们的选择使得：若 $i\in R_0$，则 $\theta(\alpha^i)=0$，若 $i\in R_1$，则 $\theta(\alpha^i)=1$. 最后，我们有 $\theta(\alpha^0)=(n-1)/2$，这就证明了定理.

现在，我们借助于 θ 构造一个 (0, 1)-矩阵 C（称为循环矩阵），它的第一行为 θ，其余的行由 θ 的全部循环移位充当. 若 $n\equiv 1 \pmod 8$，则令 $\mathbf{c}:=(00\cdots 0)$，若 $n\equiv -1 \pmod 8$，则令 $\mathbf{c}:=(11\cdots 1)$，定义

$$G=\begin{bmatrix} 1 & 1\cdots 1 \\ \mathbf{c}^T & C \end{bmatrix}$$

由定理 6.9.3，G 的行(显然并不独立)生成一个长为 $n+1$ 的二元 QR 码．我们用 n 阶射影直线中的点 ∞，0，1…，$n-1$ 来表示码字的坐标位置．奇偶校验位放在最前面，记号为∞．涉及∞的算术运算，我们采用通常的约定．群 PSL(2, n) 由全体变换 $x \to (ax+b)/(cx+d)$ 组成，其中 $a, b, c, d \in \mathbb{F}_n$ 且 $ad-bc=1$．不难验证这个群的生成元为 $S: x \to x+1$ 和 $T: x \to -x^{-1}$．显然，S 是对∞以外的位置的一个循环移位，且保持∞不动．由 QR 码的定义，S 保持扩充码不变，为了检验 T 对扩充 QR 码的影响，我们只需分析 T 如何改变 G 的行．证明 T 把 G 的一行映为 G 中至多三行的线性组合是一个简单(但可能有点繁琐)的练习(做不出的读者可参见[42])．因此，S 和 T 都保持扩充 QR 码不变．这就证明了下面的定理．

(6.9.4)定理． 长为 $n+1$ 的扩充二元 QR 码的自同构群包含 PSL(2, n)．

我们前面提到过的扩充码的修正定义，保证定理 6.9.4 对非二元情形也正确(参见[46])．

(6.9.5)推论． 二元 QR 码中的极小重量码字满足定理 6.9.2 的条件．

证明．证明与推论 6.6.8 相同．在此我们利用 PSL(2, n) 传递这一事实，因而极小重量是奇数． □

例．(a) 设 $q=2$，$n=7$，我们有

$$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1).$$

取 $g_0(x)$ 为生成元．定理 6.9.3 规定选择的 α 使得 $x+x^2+x^4$ 也是一个生成元，因此 $g_0(x)=1+x+x^3$．当然，这个码是(完全的)[7, 4] Hamming 码(见 § 3.3 和定理 6.3.1)．

(b) 设 $q=2$，$n=23$，我们有

$$x^{23}-1=(x-1)(x^{11}+x^9+x^7+x^6+x^5+x+1)$$
$$(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1).$$

仍取 $g_0(x)$ 为 $\theta(x)$ 的倍式，即

$$x^{11}+x^9+x^7+x^6+x^5+x+1.$$

由推论 6.9.5，相应的 QR 码 C 的极小距离 $\geqslant 7$.

因为 $\sum_{i=0}^{3}\binom{23}{i}=2^{11}$ 及 $|C|=2^{12}$，所以 $d=7$，且由 (3.1.6) C 是完全码. 由于 § 4.2 中的二元 Golay 码是唯一的，所以我们证明了它实际上是一个 QR 码.

我们将另外几个例子留作练习 (§ 6.11).

§ 6.10 评　注

有兴趣了解迹函数和幂等元(在证明中它们起到了重要作用)的读者可阅读[46,第 15 章].

BCH 码的推广将在第 8 章中讨论. 关于 BCH 码的重量、维数、覆盖半径等均有大量文献. 我们提一下 Carlitz-Uchiyam 界，它依赖于 A. Weil 证明的一个深刻的数论定理. 关于这个界，请读者参考[42]. 对于 QR 码到字长 n 为素数幂的推广，其理论与 § 6.9 相似. 我们建议参考 J. H. van Lint 和 F. J. MacWilliams 的论文 (1978, [45]).

§6.11 问　题

6.11.1. 证明三元[4, 2] Hamming 码是负循环码.

6.11.2. 决定二元[15, 11] Hamming 码的幂等元.

6.11.3. 证明定义 4.5.6 中的 r 阶二元 Reed-Muller 码等价于一个扩充循环码.

6.11.4. 构造一个长为 26，设计距离为 5 的三元 BCH 码.

6.11.5. 设 α 是 $\mathbf{F}_{2^5}$ 的一个本原元，满足 $\alpha^5=\alpha^2+1$. 利用一个长为 31、设计距离为 5 的狭义 BCH 码进行编码. 我们收到字

(1001 0110 1111 0000 1101 0101 0111 111).

试用 § 6.7 的方法译该消息.

6.11.6. 设 β 是 $\mathbf{F}_{2^m}$ 的一个本原元. 考虑一个长为 $n = 2^m - 1$ 的二元 BCH 码 C,其生成元 $g(x)$满足 $g(\beta) = g(\beta^{-1}) = 0$ 证明C的极小距离至少是 5.

6.11.7. 设C是 $\mathbf{F}_q$ (q 是奇数) 上的一个 $[q+1, 2, d]$ 码, 证明 $d < q$ (即C不是 MDS 码,参见(5.2.2)).

6.11.8. 证明三元 [11, 6] QR 码是完全的(它等价于 § 4.3 中的码).

6.11.9. 决定长为 47 的二元 QR 码的极小距离.

6.11.10. 决定所有单一纠错的完全 QR 码.

6.11.11. 在下述意义下推广 § 6.9 的思想. 设 $e > 2$, n 是一个使 $e|(n-1)$ 的素数, q 是一个素数的幂, 满足 $q^{(n-1)/e} \equiv l(\mathrm{mod}\ n)$. 用 e 次幂代替 $\mathbf{F}_n$ 中的平方元,证明定理 6.9.2 (i) 可推广到 $d^e > n$. 决定长为 31 的二元三次剩余码的极小距离.

6.11.12. 设m是一个奇数, $n = 2^m - 1$, α 是 $\mathbf{F}_{2^m}$ 的一个本原元. 又设 $g(x)$是 $x^n - 1$ 的一个因子,满足 $g(\alpha) = g(\alpha^5) = 0$. 用两种方法证明,生成元为 $g(x)$ 的二元循环码的极小距离 $\geqslant 4$:

(a) 应用本章的一个定理;

(b) 通过证明 $1 + \xi + \eta = 0$ 和 $1 + \xi^5 + \eta^5 = 0$,其中 $\xi, \eta \in \mathbf{F}_{2^m}$ 是不可能的.

6.11.13. 证明三元 Golay 码有负循环表示.

第七章 完全码与均匀覆盖码

§7.1 Lloyd 定理

在本章中,我们只考虑二元码,这对于了解编码理论这一方面的内容完全足够了. 只要稍加改变,几乎所有的讨论都可以在任意域 $\mathbf{F}_q$ 上进行. 随着时间的推移,许多研究完全码以及与之有关的问题的方法已得到发展,其中最精彩的可能就是我们将在下节中讨论的代数方法.对于二元 e-纠错完全码存在性的一个较强的必要条件,我们将用一种全新的方法,给出非常初等的证明. 这个定理(对于 $q=2$)首先由 S. P. Lloyd (1957) 用解析方法所证明. 尽管后来有许多作者推广了这个定理(见[44]),但我们仍将其称为 Lloyd 定理. 本节所给的证明属于 D. M. Cvetković 和 J. H. van Lint (1977,[17]).

(7.1.1) 定义. 如下定义一个 2^k 阶方阵 A_k, A_k 的行标和列标用从 0 到 2^k-1 的二进制数表示, 如果 i 和 j 的二进制表示的 Hamming 距离为 1,则元素 $A_k(i,j)=1$,否则 $A_k(i,j)=0$.

由(7.1.1)我们立即可得

$$A_{k+1}=\begin{pmatrix} A_k & I \\ I & A_k \end{pmatrix}. \tag{7.1.2}$$

(7.1.3)引理: *A_k 的特征值是* $-k+2j(0\leqslant j\leqslant k)$, *而* $-k+2j$ *的重数为* $\binom{k}{j}$.

证明. 用归纳法证明. 对于 $k=1$, 结论易证. 设列向量 $\mathbf{x}$ 是 A_k 的属于特征值 λ 的特征向量,由(7.1.2)我们有

$$A_{k+1}\begin{pmatrix}\mathbf{x}\\ \mathbf{x}\end{pmatrix}=(\lambda+1)\begin{pmatrix}\mathbf{x}\\ \mathbf{x}\end{pmatrix},$$

$$A_{k+1}\begin{pmatrix}\mathbf{x}\\-\mathbf{x}\end{pmatrix}=(\lambda-1)\begin{pmatrix}\mathbf{x}\\-\mathbf{x}\end{pmatrix}.$$

再由二项式系数的性质即知引理成立. □

在证明主要定理时将遇到三对角矩阵，而本节最困难的部分就是确定这种矩阵的特征值. 为使概念简洁我们采用下面的定义.

(7.1.4)定义. 矩阵 $Q_e=Q_e(a,b)$ 是一个三对角矩阵，其元素

$$(Q_e)_{i,i}:=a,\ 0\leqslant i\leqslant e,$$
$$(Q_e)_{i,i+1}:=b-i,\ 0\leqslant i\leqslant e-1,$$
$$(Q_e)_{i,i-1}:=i,\ 1\leqslant i\leqslant e.$$

进一步，定义

$$P_e:=P_e(a,b):=\left[\begin{array}{c|c} Q_{e-1}(a,b) & \begin{matrix}1\\1\\\vdots\\1\end{matrix} \\ \hline 0\ 0\cdots 0\ e & 1\end{array}\right].$$

它们的行列式分别记作 $\bar{Q}_e$ 和 $\bar{P}_e$.

(7.1.5)引理. 设 $\Psi_e(x)$ 是(1.2.1)和(1.2.15)中定义的 Krawtchouk 多项式 $K_e(x-1;n-1,2)$. 那么

$$\bar{P}_e(2y-n,n)=(-1)^e e!\Psi_e(y).$$

证明. 将 $\bar{Q}_e$ 按最后一行展开，有

$$\bar{Q}_e=(a+e)\bar{Q}_{e-1}-e(b-e+1)\bar{Q}_{e-2}.$$

把所有列加到最后一列上，再按最后一行展开，则得

$$\bar{Q}_e=(a+e)\bar{Q}_{e-1}-e(a+b)\bar{P}_{e-1}.$$

又将 $\bar{P}_e$ 也按最后一行展开，得

$$\bar{P}_e=\bar{Q}_{e-1}-e\bar{P}_{e-1}.$$

由这些关系式我们得到如下递推关系:

$$\bar{P}_{e+1}=(a-1)\bar{P}_e-e(b-e)\bar{P}_{e-1}. \tag{7.1.6}$$

容易验证引理的断言对 $e=1$ 和 $e=2$ 成立. 从(1.2.9)与(7.1.6)可见断言中的两个多项式满足同一递推关系，因而引理得证. □

我们还需要一个关于特征值的较为简单的引理.

(7.1.7)引理. 设 A 是形如

$$A=\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1k} \\ A_{21} & A_{22} & \cdots & A_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ A_{k1} & A_{k2} & \cdots & A_{kk} \end{bmatrix}$$

的 m 阶方阵，其中 A_{ij} 是 $m_i \times m_j$ 矩阵 $(i=1,2,\cdots,k; j=1,2,\cdots,k)$. 假定对于每一个 i 和 j,矩阵 A_{ij} 的行和为常数 b_{ij}. 令 B 是以 b_{ij} 为元素的矩阵,则 B 的每一个特征值必是 A 的特征值.

证明. 设 $B\mathbf{x}=\lambda\mathbf{x}$,其中 $\mathbf{x}=(x_1,x_2,\cdots,x_k)^T$. 令

$$\mathbf{y}:=(x_1,x_1,\cdots,x_1,x_2,x_2,\cdots,x_2,\cdots,x_k,x_k,\cdots,x_k)^T,$$

其中每个 x_i 重复 m_i 次. 由 B 的定义显然有 $A\mathbf{y}=\lambda\mathbf{y}$. □

现在我们来讨论著名的 Lloyd 定理,它将有一些重要的推论.

(7.1.8) 定理. 如果存在一个长为 n 的二元完全 e-纠错码，那么 $\Psi_e(x)$ 的 e 个不同的零点均取自整数 $1,2,\cdots,n$.

证明. Krawtchouk 多项式的一个熟知性质是它的零点互不相同(见(1.2.13)). 为证明这些零点都是整数,假定 C 是一个如定理所述的码. 考虑矩阵 A_n(见(7.1.1)). 按如下方式重排 A_n 的行和列：先取下标对应于 C 中码字的行和列，然后依次取下标对应于 $C_i:=\{\mathbf{x}\in\mathbb{F}_2^n \mid d(\mathbf{x},C)=i\}$, $1\leqslant i\leqslant e$, 中的字的那些行和列. 由于 C 是完全码，所以 A_n 可被分成一个形如引理 7.1.7 的分块矩阵,而现在

$$B=\begin{bmatrix} 0 & n & 0 & 0 & 0 & \cdots\cdots\cdots\cdots & 0 \\ 1 & 0 & n-1 & 0 & 0 & \cdots\cdots\cdots\cdots & 0 \\ 0 & 2 & 0 & n-2 & 0 & \cdots\cdots\cdots\cdots & 0 \\ & & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \\ 0 & \cdots\cdots & \cdots\cdots & 0 & e-1 & 0 & n-e+1 \\ 0 & \cdots\cdots & & 0 & 0 & e & n-e \end{bmatrix}.$$

在 $\det(B-xI_{e+1})$ 中作代换 $x=n-2y$, 得

$$\det(B - xI_{e+1}) = 2y\bar{P}_e(2y - n, n).$$

由引理 7.1.3,7.1.5 和 7.1.7 知本定理成立. □

本节所给的证明未能进一步阐明 Ψ_e 的性质(例如, Ψ_e 的零点有何组合意义?),但这是一个完全初等的证明(除了不可避免地运用了 Krawtchouk 多项式的性质以外). 在 § 7.5 中我们将利用定理 7.1.8 找出所有的二元完全码.

§ 7.2 码的特征多项式

考虑一个长为 n 的二元码 C. 在(3.5.1)中我们定义了码的重量分布, 在 (5.3.2) 中又把这个概念推广为距离分布或内分布 $(A_i)_{i=0}^n$. 对应这一序列有**距离计数子**

$$(7.2.1) \qquad A_C(z) := \sum_{i=0}^{n} A_i z^i = |C|^{-1} \sum_{\substack{\mathbf{u}\in C\\ \mathbf{v}\in C}} z^{d(\mathbf{u},\mathbf{v})}.$$

为了得到更多有关距离的信息,我们定义一个矩阵 B(以 $\mathscr{R} = \mathbf{F}_2^n$ 中的元记其行标,以 $0,1,\cdots,n$ 记其列标),其中

$$(7.2.2) \qquad B(\mathbf{x},i) := |\{\mathbf{c}\in C \mid d(\mathbf{x},\mathbf{c}) = i\}|,$$

称 B 为 C 的**外分布**. 把 B 的第 $\mathbf{x}$ 行记为 $B(\mathbf{x})$,有

$$(7.2.3) \qquad (A_0, A_1, \cdots, A_n) = |C|^{-1} \sum_{\mathbf{x}\in C} B(\mathbf{x}),$$

以及

$$(7.2.4) \qquad \mathbf{x}\in C \Longleftrightarrow B(\mathbf{x},0) = 1.$$

(7.2.5)定义. 码 C 称为**正则码**, 如果 B 的那些在位置 0 上的元素是 1 的行都相等. C 称为**完全正则码**,如果

$$\forall_{\mathbf{x}\in\mathscr{R}}\forall_{\mathbf{y}\in\mathscr{R}}[(\rho(\mathbf{x},C) = \rho(\mathbf{y},C)) \Rightarrow (B(\mathbf{x}) = B(\mathbf{y}))],$$

其中 $\rho(\mathbf{x},C)$ 是 $\mathbf{x}$ 到 C 的距离.

注意,若码 C 是正则的, 并且 $\mathbf{0}\in C$, 则 C 的重量计数子等于 $A_C(z)$.

为了研究矩阵 B,我们先引入某种代数(见 1.1.11)).

(7.2.6)定义. 设G是一个加群，$\mathbf{F}$是域，那么群代数$\mathbf{F}G$（或$(\mathbf{F}G, \oplus, *)$）是$\mathbf{F}_2$上以G中元素为基的向量空间．其中加法为$\oplus$，而乘法$*$的定义如下：

$$\sum_{g\in G}\alpha(g)g*\sum_{h\in G}\beta(h)h:=\sum_{k\in G}\Big(\sum_{g+h=k}\alpha(g)\beta(h)\Big)k.$$

有些作者宁愿引入一个外加的记号z，并定义形式乘法如下：

$$\sum_{g\in G}\alpha(g)z^g*\sum_{h\in G}\beta(h)z^h:=\sum_{k\in G}\Big(\sum_{g+h=k}\alpha(g)\beta(h)\Big)z^k.$$

我们取G为$\mathscr{R}=\mathbf{F}_2^n$，并令$\mathbf{F}=\mathbf{C}$，所得的代数记为$\mathscr{A}$．为了不致使$G$中的加法与$\mathscr{A}$中元素的加法相混淆，我们把群代数中的元写成形状$\bigoplus_{\mathbf{x}\in\mathscr{R}}\alpha(\mathbf{x})\mathbf{x}$．如果$S$是$\mathscr{R}$的一个子集，则把$S$与$\mathscr{A}$中的元素$\bigoplus_{\mathbf{x}\in S}\mathbf{x}$等同起来（也就是说，这个元素也记作$S$）．我们分别引入具有固定重量的字组成的集合和中心为0的球这两个概念：

(7.2.7) $$Y_i:=\{\mathbf{x}\in\mathscr{R}\mid w(\mathbf{x})=i\},$$

(7.2.8) $$S_j:=\{\mathbf{x}\in\mathscr{R}\mid w(\mathbf{x})\leqslant j\}.$$

若C是具有外分布B的码，则以上约定给出

(7.2.9) $$Y_i*C=\bigoplus_{\mathbf{x}\in\mathscr{R}}B(\mathbf{x},i)\mathbf{x}.$$

如果用$D(\mathbf{x},j)$记C中与$\mathbf{x}$的距离至多为j的码字数$\Big($即$D(\mathbf{x},j)=\sum_{i\leqslant j}B(\mathbf{x},i)\Big)$，那么

(7.2.10) $$S_j*C=\bigoplus_{\mathbf{x}\in\mathscr{R}}D(\mathbf{x},j)\mathbf{x}.$$

设χ是$\mathbf{F}_2$的特征标，这里$\chi(1)=-1$．对每个$\mathbf{u}\in\mathscr{R}$，定义映射$\chi_{\mathbf{u}}:\mathscr{R}\to\mathbf{C}$如下

(7.2.11) $$\forall_{\mathbf{v}\in\mathscr{R}}[\chi_{\mathbf{u}}(\mathbf{v}):=\chi(\langle\mathbf{u},\mathbf{v}\rangle)=(-1)^{\langle\mathbf{u},\mathbf{v}\rangle}],$$

也就是说，如果$\mathbf{u}\perp\mathbf{v}$则$\chi_{\mathbf{u}}(\mathbf{v})=1$，否则$\chi_{\mathbf{u}}(\mathbf{v})=-1$.

把这个映射扩充为群代数 $\mathscr{A}$ 上的线性函数:

(7.2.12) $$\chi_{\mathbf{u}}(\sum\alpha(\mathbf{x})\mathbf{x}):=\sum\alpha(\mathbf{x})\chi_{\mathbf{u}}(\mathbf{x}).$$

由定义立即可得下面的两个结论，其证明留给读者作为简单的练习.

(7.2.13) $$\forall_{\mathbf{u}\in\mathscr{R}}\forall_{A\in\mathscr{A}}\forall_{B\in\mathscr{A}}[\chi_{\mathbf{u}}(A*B)=\chi_{\mathbf{u}}(A)\chi_{\mathbf{u}}(B)],$$

(7.2.14) $$(\chi_0(S)=2^n \text{ 并且} \forall_{\mathbf{u}\neq 0}[\chi_{\mathbf{u}}(S)=0])\Longleftrightarrow S=S_n.$$

引理 5.3.1 的结果(现在 $q=2$)可以写成

(7.2.15) $$\chi_{\mathbf{u}}(y_k)=K_k(w(\mathbf{u})).$$

由此,如果 $w(\mathbf{u})=x$,那么

(7.2.16) $$\chi_{\mathbf{u}}(S_i)=\sum_{k=0}^{i}K_k=\Psi_i(x).$$

(见(1.2.15)).

设 C 是一个码. 考虑数

$$C_i:=|C|^{-1}\sum_{\mathbf{u}\in Y_i}\chi_{\mathbf{u}}(C).$$

前面我们已遇到过这些数. 若 C 是线性码,则定理 3.5.3 的证明告诉我们: C_i 就是 $C^\perp$ 中重 i 的码字数. 若 C 非线性，我们仍然可以考虑数 C_i 并继续定理 3.5.3 的证明,进而发现

$$2^{-n}|C|\sum_{i=0}^{n}C_i(1-z)^i(1+z)^{n-i}$$

是 C 的重量记数子. 这个计数子与借助 x 定义的数 C_i 之间的关系是 MacWilliam 关系式的非线性形式.

现在,我们利用特征标 χ 定义另一个数列.

(7.2.17)定义. $B_i:=|C|^{-2}\sum_{\mathbf{u}\in Y_i}|\chi_{\mathbf{u}}(C)|^2, 0\leqslant i\leqslant n$,称为码 C 的**特征数**.

如前可见,当 C 是线性码时,B_i 是 $C^\perp$ 中重为 i 的码字数. 令 $N(C):=\{i|1\leqslant i\leqslant n, B_i\neq 0\}$, 定义码 C 的**特征多项式** F_C 如下

(7.2.18) $$F_C(x):=2^n|C|^{-1}\prod_{i\in N(C)}\left(1-\frac{x}{i}\right).$$

(7.2.19)定理. 设 $\alpha_0,\alpha_1,\cdots,\alpha_n$ 是多项式 F_C 的 Krawtchouk 展式的系数，那么在 $\mathscr{A}$ 中有

$$\sum\alpha_i Y_i * C = S_n.$$

证明. 设 $\mathbf{u}\in\mathscr{R}, w(\mathbf{u})=j$. 根据(7.2.13)和(7.2.15)得

$$\chi_{\mathbf{u}}(\sum\alpha_i Y_i * C) = \chi_{\mathbf{u}}(\sum\alpha_i Y_i)\chi_{\mathbf{u}}(C) = \chi_{\mathbf{u}}(C)\sum\alpha_i K_i(j)$$
$$= \chi_{\mathbf{u}}(C)F_C(j).$$

若 $\mathbf{u}\neq\mathbf{0}$，根据 F_C 的定义知上式右边为 0，若 $\mathbf{u}=\mathbf{0}$，则右边为 2^n. 再由(7.2.14)知断言成立. □

(7.2.20)推论. 若 $\alpha_0,\alpha_1,\cdots,\alpha_n$ 是 F_C 的 Krawtchouk 展式的系数，则对于 $\mathbf{u}\in\mathscr{R}$ 有

$$\sum_{i=0}^{n}\alpha_i B(\mathbf{u},i) = 1.$$

证明. 用(7.2.9). □

(7.2.21)定义. 数 $s:=|N(C)|$ 称为 C 的外距离.

注意，若 C 是线性的，则 s 是出现在 $C^\perp$ 中的非零重量的数目. 另一方面，推论 7.2.20 证明了任意码 C 的覆盖半径 $\rho(C)$（见(3.14)）至多为 s，因此，称 s 为 C 的外距离是毫不奇怪的.

§7.3 均匀覆盖码

本节我们讨论完全码（见(3.1.5)）的推广. 如果 C 是 e-纠错完全码，那么在 $\mathscr{A}$ 中有 $S_e * C = S_n$. 现在考虑 $d\geqslant 2e+1$ 以及 $\rho(C)=e+1$ 的码 C.（若 $d=2e+3$，则 C 就是完全码.）这时，以码字为中心，$e-1$ 为半径的所有球互不相交，且每个不在任何球内的字至少与一个码字的距离为 e 或 $e+1$.

(7.3.1)定义. 设 C 是一个码并且 $d\geqslant 2e+1, \rho(C)=e+1$. 若每个满足 $\rho(\mathbf{u},C)\geqslant e$ 的字 $\mathbf{u}$ 恰好与 r 个码字的距离为 e 或 $e+1$，则称 C 是一个参数为 r 的均匀覆盖码.

如果 $r=1$，那么 C 就是一个完全 $(e+1)$-纠错码. 若字 $\mathbf{u}$ 使得 $\rho(\mathbf{u},C)=e$，则 $\mathbf{u}$ 恰与一个码字的距离为 e. 设 $\rho(\mathbf{u},C)=$

$e+1$,不失一般性,取 $\mathbf{u}=\mathbf{0}$,那么与 $\mathbf{u}$ 的距离为 $e+1$ 的码字具有重量 $e+1$,由于它们相互之间的距离必须$\geqslant 2e+1$,所以有

$$(7.3.2) \qquad r \leqslant \frac{n}{e+1}.$$

若 $r=\left\lfloor\frac{n}{e+1}\right\rfloor$,则这个码又叫做*近完全码*. 容易验证 C 满足带等号的 Johnson 界(5.2.16). J.-M. Goethals 和 H. C. A. van Tilborg 在文章[25]中对(7.3.1)作了推广,取代 r 的是与 $\rho(\mathbf{u},C)=e$ 或 $e+1$ 有关的两个数.

(7.3.3)定理. *设 C 是一个码且* $\rho(C)=e+1, d\geqslant 2e+1$, *则 C 是一个参数为 r 的均匀覆盖码当且仅当在 $\mathscr{A}$ 中有*

$$\left\{Y_0\oplus Y_1\oplus\cdots\oplus Y_{e-1}\oplus\frac{1}{r}(Y_e\oplus Y_{e+1})\right\}*C=S_n.$$

证明. 由(7.2.2),(7.2.9)和(7.3.1)即得. □

(7.3.4)定理. *设 C 是一个码且* $\rho(C)=e+1, d\geqslant 2e+1$, *则 C 是一个参数为 r 的均匀覆盖码当且仅当 C 的特征多项式的次数为* $s=e+1$, Krawtchouk *系数为*

$$\alpha_0=\alpha_1=\cdots=\alpha_{e-1}=1, \alpha_e=\alpha_{e+1}=\frac{1}{r}.$$

证明. (i)充分性由定理 7.2.19 和定理 7.3.3 可得.

(ii) 现在设 C 是均匀覆盖码.我们知道 F_C 的次数 $s\geqslant e+1$. 令 $F(x):=\sum_{i=0}^{e+1}\alpha_i K_i(x)$, 其中 $\alpha_0=\alpha_1=\cdots=\alpha_{e-1}=1$, $\alpha_e=\alpha_{e+1}=\frac{1}{r}$. 如果 $\mathbf{u}\in\mathscr{R}$, $w(\mathbf{u})=j\neq 0$, $\chi_{\mathbf{u}}(C)\neq 0$, 那么由(7.2.13)得 $F(j)=0$. 因此, 根据(7.2.18)可知 $F_C(x)$ 整除 $F(x)$. 所以 $s=e+1$ 而 $F(x)=aF_C(x)$, 对某 a. 以 $x=0$ 代入即知 $a=1$(再次运用定理 7.3.3). □

下面是定理 7.3.4 的另一表述.

(7.3.5)定理. *如果存在一个参数为 r 的均匀覆盖码 C,其中* $\rho(C)$

$= e+1, d \geqslant 2e+1$，那么多项式

$$F(x):=\sum_{i=0}^{e-1}K_i(x)+\frac{1}{r}[K_e(x)+K_{e+1}(x)]$$

在 $[1,n]$ 之间有 $e+1$ 个不同的整数根，并且 $F(0)=2^n|C|^{-1}$.

首先，我们看到，若 C 是完全码，即 $d=2e+3$，则由(1.2.15)知 $r=1, F(x)=\Psi_{e+1}(x)$，而定理 7.3.5 就是 Lloyd 定理 7.1.8.

其次，对 $F(0)$ 的要求可以写成

$$(7.3.6)\qquad |C|\left\{\sum_{i=0}^{e-1}\binom{n}{i}+\frac{1}{r}\binom{n+1}{e+1}\right\}=2^n.$$

如果 $r=1$ 和 $r=\left\lfloor\frac{n}{e+1}\right\rfloor$，那么上式分别变成(3.1.6)和(5.2.16).

事实上，若把 r 换成与满足 $\rho(\mathbf{u},C)\geqslant e$ 的字 $\mathbf{u}$ 相距 e 或 $e+1$ 的码字数的平均值，则(7.3.6)仍然成立.

一般地，我们很难利用定义去检验一个给定的码是否为均匀覆盖码.

现在，我们考虑一种特殊情况，即 C 为线性码且 $e=1$ 的情形. 若 C 为均匀覆盖码，则 C 的特征多项式的次数必为 2（根据定理 7.3.4)，也就是说，在 $C^\perp$ 中仅有两个非零重量 w_1 和 w_2 出现. 假定 $C^\perp$ 是这样一个2-重量码，其重量计数子为

$$A_{C^\perp}(z)=1+N_1z^{w_1}+N_2z^{w_2}.$$

考虑 MacWilliams 关系(见 § 7.2)，并以

$$\sum_{k=0}^{\infty}K_k(x)z^k$$

代替 $(1+z)^{n-x}(1-z)^x$（见(1.2.3)). 由于已假定 C 的极小距离 $d\geqslant 3$，因此从 z^0, z^1, z^2 的系数我们可得三个方程:

$$1+N_1+N_2=2^n|C|^{-1},$$

$$K_k(0)+N_1K_k(w_1)+N_2K_k(w_2)=0,(k=1,2).$$

由定义，我们有 $F_C(w_1)=F_C(w_2)=0$ 以及 $F_C(0)=2^n|C|^{-1}$.

对于 $F_C(x)$ 的 Krawtchouk 展式的系数 $\alpha_0,\alpha_1,\alpha_2$，运用(1.2.7)可得

$$\alpha_0+\alpha_1 n+\alpha_2\binom{n}{2}=2^n|C|^{-1},$$

$$\alpha_0+\alpha_1(n-2w_i)+\alpha_2\left\{2w_i^2-2nw_i+\binom{n}{2}\right\}=0,(i=1,2).$$

将这几个方程与 N_1,N_2 满足的方程相比较，即得 $\alpha_0=1$. 再定义

$$r:=2(n+1)w_1-2w_1^2-\frac{1}{2}n(n+1).$$

由上可见，若 $w_1+w_2=n+1$，则 $\alpha_1=\alpha_2=\frac{1}{r}$. 因此，我们证明了1-纠错均匀覆盖码的一个特征性质:

(7.3.7)定理. 设 C 是一个线性码且 $\rho(C)=2,d\geqslant 3$. 那么 C 为均匀覆盖码当且仅当 $C^\perp$ 是一个具有非零重量 w_1 和 w_2 的 2-重量码，并且 $w_1+w_2=n+1$.

文献[25]证明，若采用均匀覆盖码的更一般性定义，则可取消 $w_1+w_2=n+1$ 这一限制. 对于 $e>1$ 且 $C^\perp$ 有 $e+1$ 个非零重量的码 C，本定理同样成立.

§7.4 均匀覆盖码的例子

(7.4.1) Hadamard 码(见§4.1).

考虑 (12, 24, 6) Hadamard 码. 删去第一分量得到一个(11,24,5)码 C. 显然地，任意字 $\mathbf{z}$ 至多与4个码字的距离为2或3. 如果这种情况发生，则有如下形状(恢复±记号并适当取某些列的−1倍):

$\mathbf{z}=--\ \ +++\ \ +++\ \ +++,$

$\mathbf{x}_1=++\ \ +++\ \ +++\ \ +++,$

$\mathbf{x}_2=--\ \ ---\ \ +++\ \ +++,$

$\mathbf{x}_3 = --\ \ +++\ \ ---\ \ +++,$

$\mathbf{x}_4 = --\ \ +++\ \ +++\ \ ---.$

这说明原来的 12 阶 Hadamard 矩阵有四个行：$(+,\mathbf{x}_1)$，$(-,\mathbf{x}_2)$，$(-,\mathbf{x}_3)$，$(-,\mathbf{x}_4)$. 由这四个向量的线性组合得到的行向量 $(-4,-4,-4,0,0,\cdots,0)$ 必与这个 Hadamard 矩阵的其余行正交，这显然是不可能的. 因此，字 $\mathbf{z}$ 至多只能与 3 个码字的距离为 2 或 3. 由(7.3.6)可知，当 $\mathbf{z}$ 满足 $\rho(\mathbf{z},C)>1$ 时，与 $\mathbf{z}$ 相距 2 或 3 的码字数的平均值恰为 3，所以这个数总是 3. 这证明了 C 是参数为 $r=3$ 的均匀覆盖码. 本例中 C 是非线性的.

(7.4.2)删减 RM 码

设 V 是 $\mathbf{F}_2$ 上 6 维向量空间，令 W 是二次方程 $x_1x_2+x_3x_4+x_5x_6=0$ 在 $V\backslash\{\mathbf{0}\}$ 中的 35 个解. 以它们为列组成一个 6×35 矩阵 G. 类似于 § 4.5，可见 G 的第 i 行是 W 与方程 $x_i=1(1\leqslant i\leqslant 6)$ 所确定的超平面之交的特征函数. 所以线性组合 $\mathbf{a}^TG(\mathbf{a}\in V)$ 的重量是方程组

$$\begin{cases} x_1x_2+x_3x_4+x_5x_6=0, \\ \sum_{i=1}^{6} a_ix_i=1 \end{cases}$$

的解数. 不失一般性，取 $a_1=1$（除 $\mathbf{a}=\mathbf{0}$ 外）. 作仿射变换

$$y_2=x_2,\ y_3=x_3+a_4x_2,\ y_4=x_4+a_3x_2,$$
$$y_5=x_5+a_6x_2,\ y_6=x_6+a_5x_2$$

（这是一个可逆变换）. 我们来计算方程

$$(1+a_2+a_3a_4+a_5a_6)y_2+y_3y_4+y_5y_6=0$$

的解数. 若 y_2 的系数为 1，则解数为 16，若 y_2 的系数为 0，则解数为 20. 因此以 G 为奇偶校验矩阵的码 C 的对偶码 $C^\perp$ 是一个具有重量 16 和 20 的 2-重量码. 又因为 W 中的向量互不相等，所以 C 的极小距离 $d\geqslant 3$. 根据(7.2.21)后的注记我们有 $\rho(C)=2$，所以，由(7.3.6)和定理(7.3.7)，C 是参数为 $r=10$ 的均匀覆盖码. 这个方法同样可以用于更高维的空间.

(7.4.3) Preparata 码

1968 年，F. P. Preparata[57] 引进了一类非线性双纠错码，并证明它们具有许多有趣的性质．他的定义建立在 Hamming 码与 2-纠错 BCH 码的结合之上．对这个码的分析涉及许多繁琐的计算（见[11]）．R. D. Baker 和 R. M. Wilson 发现（未发表），Preparata 码可以用简单得多的方式予以定义，我们下面的定义和分析就是基于这个建议的．

下面假定 m 是奇数（$m \geq 3$），$n = 2^m - 1$．我们将定义一个长为 $2n + 2 = 2^{m+1}$ 的码 $\bar{\mathscr{P}}$，其码字用子集对 (X, Y) 表示，其中 $X \subset \mathbb{F}_{2^m}$，$Y \subset \mathbb{F}_{2^m}$．通常，我们把对 (X, Y) 看作对应的特征函数，即长为 2^{m+1} 的(0,1)向量．

(7.4.4)定义． 长为 2^{m+1} 的扩张 Preparata 码 $\bar{\mathscr{P}}$ 由所有满足下列条件的对 (X,Y) 所组成．

(i) $|X|$ 和 $|Y|$ 是偶数，

(ii) $\sum_{x \in X} x = \sum_{y \in Y} y$，

(iii) $\sum_{x \in X} x^3 + \left(\sum_{x \in X} x\right)^3 = \sum_{y \in Y} y^3$.

Preparata 码 $\mathscr{P}$ 是由 $\bar{\mathscr{P}}$ 中的码字去掉前半部分位置 0 上的分量所得的码．

我们首先证明 $\bar{\mathscr{P}}$ 有 2^{2n-2m} 个码字．易见，满足 (i) 的 X 的取法有 2^n 种．又因为 m 是奇数，所以极小多项式 $m_3(x)$ 的次数为 m，因此长为 n，设计距离为 5 的 BCH 码的维数为 $n - 2m$．这表明对于给定的 X，方程(ii)和(iii)有 2^{n-2m} 个解 $Y \subset \mathbb{F}_{2^m}^*$．必要时，在 Y 中加上零元使之满足 (i)．这就证明了我们的断言．

其次，我们断定 $\bar{\mathscr{P}}$ 的极小距离为 6．由(7.4.4)(i)可见，极小距离应为偶数．另外，如果 (X,Y) 满足上述三条，则 (Y,X) 也是如此．假定 (X,Y_1) 和 (X,Y_2) 是两个码字，令 $Y := Y_1 \triangle Y_2$．由 (7.4.4) (ii) 和 (iii) 可得

$$\sum_{y \in Y} y = \sum_{y \in Y} y^3 = 0.$$

根据 BCH 界,这说明 $|Y| \geqslant 5$. 因此在这种情况下,两个码字的距离$\geqslant 6$. 剩下要考虑的是可能有码字 (X_1, Y_1) 和 (X_2, Y_2) 满足

$$|X_1 \triangle X_2| = |Y_1 \triangle Y| = 2.$$

令 $X_1 \triangle X_2 = \{\alpha, \beta\}$, $Y_1 \triangle Y_2 = \{\gamma, \delta\}$, 并设 X_1 中元素的和为 $s + \alpha$. 由(7.4.4)(ii) 和 (iii) 推出

$$\alpha + \beta = \gamma + \delta,$$

$$s^2(\alpha + \beta) + s(\alpha + \beta)^2 = \gamma^3 + \delta^3.$$

据此有 $(s + \gamma)^3 + (s + \delta)^3 = 0$, 即 $\gamma = \delta$, 矛盾. 这就证明了我们的断言. 事实上,我们已经证明了:

(7.4.5)定理. 长为 $2^{m+1} - 1$ 的 Preparata 码 $\mathscr{P}$ 含 2^k 个码字, 极小距离为 5. 这里 $m \geqslant 3$ 是奇数, $k = 2^{m+1} - 2m - 2$.

由(7.3.6)可见, 对于码 $\mathscr{P}$, r 的平均值是 $(2^{m+1} - 1)/3$, 而(7.3.2)表明 r 是常数且等于 $(2^{m+1} - 1)/3$, 因此 $\mathscr{P}$ 是近完全码.

若在(7.4.4)中取 $m = 3$,则得到我们在 § 4.4 中引进的 Nordstrom-Robinson 码.

注. 在(7.4.4)(iii) 中指数 3 并不是必需的,我们可以用 $s := 2^t + 1$ 代替 3, 但要求映射 $x \to x^s$ 和 $x \to x^{s-2}$ 是 $\mathbf{F}_{2^m}$ 自身上的一一对应. 有关极小距离的前半依据可用定理 6.6.3 代替. 我们把这个证明作为一个简单的练习留给读者.

§ 7.5 不存在性定理

A. Tietäväinen ([68]) 与 J. H. van Lint ([41]) 证明,在任意含素数幂个元的字母集 Q 上,当 $e > 1$ 时,Golay 码是唯一的非平凡 e-纠错完全码. M. R. Best ([7])证明: 当 $e > 2$, $e \neq 6$ 时,关于 Q 的限制可以取消, 但其证明更为复杂. 对于 $e = 1$, 我们知道, Hamming 码是 1-纠错完全码, 并且还存在非线性的 1-纠错完全码(见(7.7.4)).

1975 年，van Tilborg ([69]) 证明，当 $e > 3$ 时，不存在 e-纠错均匀覆盖码，而当 $e \leqslant 3$ 时，所有 e-纠错均匀覆盖码都是已知的. 本节我们将给出这些方法的某些思想，并用以证明上述结论. 同样，只考虑二元情况就够了.

(7.5.1)定理. 若 C 是一个 e-纠错完全码，其中 $e > 1$，那么 C 是重复码或者二元 Golay 码.

证明. 根据 Lloyd 定理 7.1.8，多项式 Ψ_e 的零点 $x_1 < x_2 < \cdots < x_e$ 是 $[1, n]$ 之间的整数. 由 Ψ_e 的定义及(1.2.8)，这些零点的 1 次和 2 次初等对称多项式为

(7.5.2)
$$\sum_{i=1}^{e} x_i = \frac{1}{2} e(n+1),$$

(7.5.3)
$$\sum_{i<j} x_i x_j = \frac{1}{24} e(e-1)\{3n^2 + 3n + 2e + 2\}.$$

注意到(7.5.2)也可以由(1.2.2)推出，并且由(1.2.2)还得

(7.5.4)
$$x_{e-i+1} = n + 1 - x_i.$$

结合(7.5.2)和(7.5.3)有

(7.5.5)
$$\sum_{i=1}^{e} \sum_{j=1}^{e} (x_i - x_j)^2 = \frac{1}{2} e^2(e-1)\left\{n - \frac{2e-1}{3}\right\}.$$

为了得到这些零点的积，我们来计算 $\Psi_e(0)$. 由(1.2.1)有

$$\Psi_e(0) = \sum_{j=0}^{e} \binom{n}{j}.$$

将此式与(3.1.6)和(1.2.8)相结合，我们发现

(7.5.6)
$$\prod_{i=1}^{e} x_i = e!\,2^l, \text{（对某整数 } l\text{）}.$$

用同样的方法计算 $\Psi_e(1)$ 和 $\Psi_e(2)$ 可得

(7.5.7)
$$\prod_{i=1}^{e} (x_i - 1) = 2^{-e}(n-1)(n-2)\cdots(n-e),$$

(7.5.8)
$$\prod_{i=1}^{e} (x_i - 2) = 2^{-e}(n-1-2e)(n-2)(n-3)\cdots(n-e).$$

现在，从这些关系式来导出关于 $x_1, x_2, \cdots, x_e$ 的一些结论．以 $A(x)$ 记 x 的最大奇因子，那么(7.5.6)表明

$$\prod_{i=1}^{e} A(x_i) = A(e!) < e!.$$

由此即知必有两个零点 x_i 和 x_j 使得 $A(x_i) = A(x_j)(i < j)$．于是 $2x_i < x_j$，因此 $2x_1 < x_e$，并且由(7.5.4)有

$$x_e - x_1 \geqslant \frac{1}{3}(n+1). \tag{7.5.9}$$

如果固定 x_1 和 x_2，那么(7.5.5)左边当

$$x_2 = x_3 = \cdots = x_{e-1} = \frac{1}{2}(x_1 + x_e)$$

时达到最小值．

将这些值代入(7.5.5)，推出

$$(x_e - x_1)^2 \leqslant \frac{1}{2} e(e-1)\left(n - \frac{2e-1}{3}\right), \tag{7.5.10}$$

再将上式与(7.5.9)相结合，其结果为

$$n + 1 \leqslant \frac{9}{2} e(e-1). \tag{7.5.11}$$

现在考虑(7.5.7)和(7.5.8)．因为当 $x \in \mathrm{N}$ 时，$(x-1)(x-2)$ 总是偶数，所以

$$(n-1-2e)(n-1)(n-2)^2(n-3)^2\cdots(n-e)^2 \equiv 0 (\mathrm{mod} 2^{3e}). \tag{7.5.12}$$

若 $e = \frac{1}{2}(n-1)$，则 C 为重复码，而上式是显然的，现在假定 $e < \frac{1}{2}(n-1)$．设 2^{α} 是(7.5.12)左边所有因子 $n-i$（包括 $n-1-2e$）的 2 的最高幂，那么整除(7.5.12)左边的 2 的方幂至多是 $2^{3\alpha+3e-3}$，因此 $\alpha \geqslant \frac{1}{3}e + 1$．于是有

$$n > 2^{1+\frac{1}{3}e}. \tag{7.5.13}$$

若 e 较大，则(7.5.13)与(7.5.11)互相矛盾．由(7.5.11)，e 较小时 n 也较小．对于较小的 e 是容易检验的．事实上，如果我们稍微准确地估计一下 n 的值，则只剩下很少的几种情况有待考虑．可以证明，$e=3$ 是唯一可能的值．实际上，$e=3$ 可以完全不用 Lloyd 定理加以处理，这一点已如问题 3.7.1 所述． □

证明所有均匀覆盖码都是已知的，可以根据同样的线索进行，但由于参数 r 的出现，我们还需要一些别的技巧．

(7.5.14)定理． 表(7.5.18)列出了全部均匀覆盖码．

证明．我们从推广的 Lloyd 定理(即定理 7.3.5)开始．用证明(7.5.10)和(7.5.13)的方法，我们可得

$$x_{e+1}-x_1\leqslant(e+1)\left(\frac{n+1}{2}\right)^{1/2},\tag{7.5.15}$$

$$n>2^{e/7}.\tag{7.5.16}$$

但用以导出(7.5.9)的论据必须加以改进．将 Ψ_e 的零点重新记为 $y_1,\cdots,y_{e+1}$，其中 $y_i=A(y_i)2^{\alpha_i}$，$\alpha_1\leqslant\alpha_2\leqslant\cdots\leqslant\alpha_{e+1}$．一方面，我们有(用 (a,b) 记 a,b 的最大公因子)：

$$\begin{aligned}\prod_{i=1}^{e}\frac{|y_i-y_{i+1}|}{y_i}&\geqslant\prod_{i=1}^{e}\frac{(y_i,y_{i+1})}{y_i}=\prod_{i=1}^{e}\frac{(A(y_i),A(y_{i+1}))2^{\alpha_i}}{y_i}\\&\geqslant\prod_{i=1}^{e}\frac{1}{A(y_i)}\geqslant\frac{1}{A(y_1\cdots y_{e+1})}\\&=\frac{A(|C|)}{A(r)A((e+1)!)}\geqslant\frac{1}{rA((e+1)!)}.\end{aligned}$$

最后一个不等式用到(7.3.6)．另一方面，又有

$$\begin{aligned}\prod_{i=1}^{e}\frac{|y_i-y_{i+1}|}{y_i}&\leqslant\frac{(x_{e+1}-x_1)^e}{y_1\cdots y_e}\leqslant\frac{n(x_{e+1}-x_1)^e}{x_1x_2\cdots x_{e+1}}\\&=\frac{n(x_{e+1}-x_1)^e}{r(e+1)!}\cdot\frac{2^{e+1}|C|}{2^n}.\end{aligned}$$

结合这两个不等式得

$$(x_{e+1}-x_1)^e \geqslant \frac{(e+1)!}{A((e+1)!)} \cdot \frac{1}{2^{e+1}} \cdot \frac{2^n}{n|C|}$$

$$\geqslant \frac{(e+1)!}{A((e+1)!)} \cdot \frac{1}{2^{e+1}} \cdot \frac{1}{n} \sum_{i=0}^{e} \binom{n}{i}$$

$$\geqslant \frac{(e+1)!}{A((e+1)!)} \cdot \frac{1}{2^{e+1}} \cdot \frac{1}{n} \binom{n}{e},$$

所以

(7.5.17)
$$(x_{e+1}-x_1)^e \geqslant \frac{(e+1)}{A((e+1)!)} \times \frac{1}{2^{e+1}}(n-1)(n-2)\cdots(n-e+1).$$

比较(7.5.15),(7.5.16)和(7.5.17)，若 $e \geqslant 3$，则只有有限个数对 (e,n) 同时满足这三个不等式． $e=1$ 与 $e=2$ 时可以很容易地利用定理 7.3.5 加以处理，而其它有限多种情形就只得分开进行分析了，最后可找出如下表所示的全部均匀覆盖码，具体细节从略(见[69])． □

(7.5.18)所有二元完全码，近完全码和均匀覆盖码表

e	n	$\|C\|$	类型	说　明
0	n	2^n	完全码	$\{0,1\}^n$
1	2^m-1	2^{n-m}	完全码	Hamming 码(以及其它码)
1	2^m-2	2^{n-m}	近完全码	缩短 Hamming 码(见(7.7.1))
1	$2^{2m-1}\pm 2^{m-1}-1$	2^{n-2m}	均匀覆盖码	见(7.4.2)
2	$2^{2m}-1$	2^{n+1-4m}	近完全码	Preparata 码
2	$2^{2m+1}-1$	2^{n-4m-2}	均匀覆盖码	BCH 码(见(7.7.2))
2	11	24	均匀覆盖码	见(7.4.1)
3	23	2^{12}	完全码	Golay 码
e	$2e+1$	2	完全码	重复码
e	e	1	完全码	$\{0\}$

§7.6 评　　注

完全码已在几个方向得到了推广（例如采用与 Hamming 距

离不同的度量以及混合的字母集等)，读者可以参看综述[44](其中包括许多参考资料).

Tietäväinen 不存在性证明的一个改进可以在[46]中找到，其中也包含许多参考资料.

有关均匀覆盖码的最完整的资料可参看[69]. 与设计理论的关系可参看[11]和[46].

如果字母集 Q 中所含元素的个数不是素数方幂，那么似乎很难确定在 Q 上是否存在未知的 2-纠错完全码，但并不是不可能的. $e=1$ 的情况看来是没有希望了.

本章所采用的许多思想方法(例如 § 7.2)都是 P. Delsarte 引入的(见[18]).

§ 7.7 问　题

7.7.1. 证明缩短二元 $[2^m-2, 2^m-m-2]$ Hamming 码是近完全码.

7.7.2. 设 C 是长 $n=2^{2m+1}-1$，设计距离 5 的 BCH 码. 直接计算与满足 $\rho(\mathbf{u},C)\geqslant 2$ 的字 $\mathbf{u}$ 距离为 3 的码字数，证明 C 是参数为 $r=\frac{1}{6}(n-1)$ 的均匀覆盖码.

7.7.3. 证明存在一个均匀覆盖码 C，使 $\bar{C}$ 是 Nordstrom-Robinson 码.

7.7.4. 设 H 是[7,4]二元 Hamming 码. 在 H 上定义 f 使 $f(\mathbf{0})=0, f(\mathbf{c})=1, \mathbf{c}\neq\mathbf{0}$. 令 C 是一个长为 15 的码，其码字为

$$\left(\mathbf{x}, \mathbf{x}+\mathbf{c}, \sum_{i=1}^{7} x_i + f(\mathbf{c})\right), \text{其中 } \mathbf{c}\in H, \mathbf{x}\in \mathbb{F}_2^7.$$

证明 C 是完全码，并且，C 不等价于任何线性码.

7.7.5. 证明二元 2-纠错完全码是平凡的.

7.7.6. 设 C 是一个长为 $n, e=1, r=6$ 的均匀覆盖码. 证明 $n=27$ 并给出 C 的构造.

第八章　Goppa 码

§8.1　引　　言

类似如定理 6.6.2 的证明，我们再次考虑一个狭义 BCH 码的奇偶校验矩阵，即

$$H=\begin{bmatrix}1 & \beta & \beta^2 & \cdots & \beta^{n-1}\\ 1 & \beta^2 & \beta^4 & \cdots & \beta^{2(n-1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & \beta^{d-1} & \beta^{2(d-1)} & \cdots & \beta^{(d-1)(n-1)}\end{bmatrix},$$

其中 β 是 $\mathbf{F}_{q^m}$ 中的一个 n 次本原单位根，而H的每一个元素看作 $\mathbf{F}_q$ 上的m维列向量(β 的存在性说明 $n|(q^m-1)$).

在定理 6.6.2 中，我们验证了H的任意 $d-1$ 列都组成一个 Vandermonde 矩阵，因此其行列式 $\neq 0$. 进而证明了最小距离至少是 d. 许多作者都注意到，如果用矩阵

$$\hat{H}=\begin{bmatrix}h_0\beta_0 & h_1\beta_1 & \cdots & h_{n-1}\beta_{n-1}\\ \vdots & \vdots & & \vdots\\ h_0\beta_0^{d-1} & h_1\beta_1^{d-1} & \cdots & h_{n-1}\beta_{n-1}^{d-1}\end{bmatrix}$$

代替 H，则同样的结论也成立，这里 $h_j\in\mathbf{F}_{q^m}^*$，β_i 是 $\mathbf{F}_{q^m}^*$ 中不同的元。若 $h_j\in\mathbf{F}_q(0\leqslant j\leqslant n-1)$，那么因子 h_j 在本质上不起作用，该码可用一个等价的码代替. 然而，如果 h_j 是 $\mathbf{F}_{q^m}^*$ 中的元，那么项 $h_j\beta_j^i$ 看作 $\mathbf{F}_q$ 上的列向量时可能与原来的元素完全不同.

我们将以这种方式考虑 BCH 码的两种推广. 虽然我们知道长的 BCH 码是劣码，但新的码类含有满足 Gilbert 界的序列，因此得到了许多有趣的性质.

§8.2 Goppa 码

设 $(c_0,c_1,\cdots,c_{n-1})$ 是长为 n,设计距离为 d 的 BCH 码中的一个码字,那么,由定义,$\sum_{i=0}^{n-1} c_i(\beta^j)^i = 0, 1 \leqslant j < d$, 其中 β 是 n 次本原单位根。我们希望将这一条件以另一方式写出。注意到

$$(8.2.1) \qquad \frac{z^n - 1}{z - \beta^{-i}} = \sum_{k=0}^{n-1} z^k(\beta^{-i})^{n-1-k} = \sum_{k=0}^{n-1} \beta^{i(k+1)} z^k,$$

可见

$$(8.2.2) \qquad \sum_{i=0}^{n-1} \frac{c_i}{z - \beta^{-i}} = \frac{z^{d-1}p(z)}{z^n - 1},$$

对某多项式 $p(z)$.

若 $g(z)$ 是任一多项式且 $g(\gamma) \neq 0$,我们定义 $1/(z-\gamma)$ 为满足 $(z-\gamma)\cdot 1/(z-\gamma) \equiv 1(\mathrm{mod}\, g(z))$的唯一的一个多项式,即

$$(8.2.3) \qquad \frac{1}{z-\gamma} = \frac{-1}{g(\gamma)}\left(\frac{g(z)-g(\gamma)}{z-\gamma}\right).$$

以上推导是下列定义的准备.

(8.2.4)定义. 设 $g(z)$ 是 $\mathbf{F}_{q^m}$ 上 t 次首 1 多项式. 令 $L = \{\gamma_0, \gamma_1,\cdots,\gamma_{n-1}\} \subset \mathbf{F}_{q^m}$, 满足 $|L| = n$ 且 $g(\gamma_i) \neq 0$, $0 \leqslant i \leqslant n-1$. 定义具有 Goppa 多项式 $g(z)$ 的 Goppa 码 $\Gamma(L,g)$ 为 $\mathbf{F}_q$ 上满足条件

$$(8.2.5) \qquad \sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} \equiv 0 \pmod{g(z)}$$

的字 $(c_0,c_1,\cdots,c_{n-1})$ 组成的集合.

易见 Goppa 码是线性码.

(8.2.6)例. 如本节开始所述,若取 Goppa 多项式 $g(z) = z^{d-1}$, 以及 $L = \{\beta^{-i} | 0 \leqslant i \leqslant n-1\}$, 其中 β 是 $\mathbf{F}_{q^m}$ 中的 n 次本原单

位根，则得到的 Goppa 码 $\Gamma(L,g)$ 是设计距离为 d 的狭义 BCH 码(见问题 8.8.2)。

为了与 § 8.1 建立联系，我们试图找出 $\Gamma(L,g)$ 的一个适当的奇偶校验矩阵. 由(8.2.5)和(8.2.3)我们看到，若把

$$\left(\frac{1}{g(\gamma_0)}\cdot\frac{g(z)-g(\gamma_0)}{z-\gamma_0},\cdots,\frac{1}{g(\gamma_{n-1})}\cdot\frac{g(z)-g(\gamma_{n-1})}{z-\gamma_{n-1}}\right)$$

的每一分量看作一个列向量，则它就是一个在某种意义下的奇偶校验矩阵. 令 $h_j:=g(\gamma_j)^{-1}$，则 $h_j\neq 0$，如果 $g(z)=\sum_{i=0}^{t}g_iz^i$，那么与(8.2.1)类似可得

$$\frac{g(z)-g(x)}{z-x}=\sum_{i+j\leqslant t-1}g_{i+j+1}x^jz^i.$$

弃掉因子 z^i，得到 $\Gamma(L,g)$ 的奇偶校验矩阵

$$\begin{bmatrix} h_0g_t & \cdots\cdots\cdots\cdots & h_{n-1}g_t \\ h_0(g_{t-1}+g_t\gamma_0) & \cdots\cdots\cdots\cdots & h_{n-1}(g_{t-1}+g_t\gamma_{n-1}) \\ \cdots\cdots\cdots & \cdots\cdots\cdots\cdots & \cdots\cdots\cdots \\ h_0(g_1+g_2\gamma_0+\cdots+g_t\gamma_0^{t-1}) & \cdots & h_{n-1}(g_1+g_2\gamma_{n-1}+\cdots+g_t\gamma_{n-1}^{t-1}) \end{bmatrix}.$$

利用线性变换，就得到了所需的矩阵

$$H=\begin{bmatrix} h_0 & \cdots & h_{n-1} \\ h_0\gamma_0 & \cdots & h_{n-1}\gamma_{n-1} \\ \cdots & \cdots & \cdots \\ h_0\gamma_0^{t-1} & \cdots & h_{n-1}\gamma_{n-1}^{t-1} \end{bmatrix}$$

(这里用到了 $g_t\neq 0$ 这一事实).

这个矩阵不象 § 8.1 中矩阵 $\hat{H}$ 那样具有广泛性，因为在 $\hat{H}$ 中，h_j 是任意的，而现在我们有 $h_j=g(\gamma_j)^{-1}$.

(8.2.7)定理. 由(8.2.4)所定义的 Goppa 码 $\Gamma(L,g)$ 的维数 $\geqslant n-mt$. 极小距离 $\geqslant t+1$.

证明. 与 BCH 码类似，由奇偶校验矩阵 H 的性质即得. □

(8.2.6)中给出的例子说明 BCH 界(对狭义 BCH 码)是定理 8.2.7 的一个特殊情况。

§ 8.3 Goppa 码的极小距离

若将我们的着眼点稍加改变，则有可能用另一种方法得到(8.2.7)，还可能得到某些改进。如前，用 $\mathscr{R}$ 记 $(\mathbf{F}_q)^n$，令 L 如(8.2.4)。定义

$$\mathscr{R}^*:=\left\{\xi(z)=\sum_{i=0}^{n-1}\frac{b_i}{z-\gamma_i}\,\middle|\,(b_0,b_1,\cdots,b_{n-1})\in\mathscr{R}\right\}.$$

再定义两个有理函数 $\xi(z)$ 和 $\eta(z)$ 的距离为

$$d(\xi(z),\eta(z)):=\|\xi(z)-\eta(z)\|,$$

其中，当 $\xi(z)$ 写成形式 $n(z)/d(z)$ 且 $(n(z),\ d(z))=1$ 时，$\|\xi(z)\|$ 表示分母 $d(z)$ 的次数。易见这是一个距离函数。并且，映射 $(b_0,\cdots,b_{n-1})\to\sum_{i=0}^{n-1}\frac{b_i}{z-\gamma_i}$ 是 $\mathscr{R}$ 到 $\mathscr{R}^*$ 上的等距同构。我们将把(8.2.5)左边看作 $\mathscr{R}^*$ 中的元素，并用上面的术语来研究 Goppa 码(即不用(8.2.3))。若 $\xi(z)=n(z)/d(z)$ 对应一个非零码字，则 $\deg d(z)\geqslant\deg n(z)+1$。而 $\xi(z)\equiv 0(\mathrm{mod}\, g(z))$ 意指 $g(z)$ 整除 $n(z)$，因此 $\deg d(z)\geqslant t+1$，于是有 $\|\xi(z)\|\geqslant t+1$。这是定理 8.2.7 的结论。

以上结论表明，如果 $d(z)$ 与 $n(z)$ 的次数之差大于 1，则可以改进对极小距离的估计。由于在 $n(z)$ 中 z^{n-1} 的系数为 $\sum_{i=0}^{n-1}b_i$，所以，若另外添加一个奇偶校验方程 $\sum_{i=0}^{n-1}b_i=0$，则对极小距离的估计可以增加 1，而维数至多减少 1。我们可将同样的想法用于其它系数。在分子 $n(z)$ 中 z^{n-s-1} 的系数为

$$(-1)^s\sum_{i=0}^{n-1}b_i\sum_{i_1\cdots i_s}{}'\gamma_{i_1}\gamma_{i_2}\cdots\gamma_{i_s}$$

(其中 Σ' 表示 $i_\nu\neq i,\nu=1,2,\cdots,s$)。这个系数是和

$$\sum_{i=0}^{n-1} b_i \gamma_i^r \ (0 \leqslant r \leqslant s)$$

的线性组合．由此可见，如果我们再加 $s+1$ 个奇偶校验方程：$\sum_{i=0}^{n-1} b_i\gamma_i^r = 0(0 \leqslant r \leqslant s)$，则可找到一个维数 $\geqslant n - tm - (1+sm)$，极小距离 $\geqslant t+s+2$ 的码．把这个码与一个用 $t+s$ 次 Goppa 多项式得到的码相比较又会怎样呢？我们说，前一方法较为优越，因为 $\sum_{i=0}^{n-1} b_i\gamma_i = 0$ 意味着 $\sum_{i=0}^{n-1} b_i\gamma_i^q = 0$，所以，一旦有 q 次出现就可以肯定维数没有减少．

应注意到，上面所简述的过程与取 Goppa 码和 BCH 码的交或多或少有些相似之处．

上述方法对二元码的情形特别有用，这就是

(8.3.1)定理． 设 $q=2$，而 $g(z)$ 无重根，那么 $\Gamma(L,g)$ 的极小距离 $\geqslant 2t+1$，其中 $t = \deg g(z)$．

证明．设 $(c_0, c_1, \cdots, c_{n-1})$ 是一个码字．定义

$$f(z) = \prod_{i=0}^{n-1} (z-\gamma_i)^{c_i},$$

那么 $\xi(z) = \sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} = f'(z)/f(z)$，这里 $f'(z)$ 是 $f(z)$ 的形式微商．在 $f'(z)$ 中只有 z 的偶数次幂出现，即 $f'(z)$ 为一完全平方．由于 $g(z)$ 必须整除 $f'(z)$，所以实际上 $g(z)^2$ 可以整除 $f'(z)$．于是，利用前面的讨论即得 $d \geqslant 2t+1$． □

当然，我们也可以把定理 8.3.1 与取 Goppa 码和 BCH 码的交这一想法联系起来．

§ 8.4 Goppa 码的渐近特性

在 § 6.6 中，我们曾指出，长的本原 BCH 码是劣码．这一事实是与定理 6.6.7 有关的．T.Kasami (1969, [39]) 证明，一族循

环码，若它们的扩张码在仿射群下不变，则对具有长度 n_i，维数 k_i，距离 d_i 的码组成的子序列 C_i，必有 $\lim\inf(k_i/n_i) = 0$ 或者 $\lim\inf(d_i/n_i) = 0$，因此这样的码也是劣码．现在我们证明 Goppa 码是一个相当大的码类．

(8.4.1)定理． 在 $\mathbf{F}_q$ 上存在一列 Goppa 码满足 Gilbert 界．

证明．先选参数 $n = q^m$，以及 t 和 d，再取 $L = \mathbf{F}_{q^m}$．我们试图在 $\mathbf{F}_{q^m}$ 上找到一个不可约多项式 $g(z)$，使得$\Gamma(L,g)$的极小距离$\geq d$．设 $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1})$ 是任一重 $j < d$ 的字，即 $\mathbf{c}$ 是 $\Gamma(L,g)$ 之外的一个字．因为 $\sum_{i=0}^{n-1} c_i/(z_i - \gamma_i)$分子的次数为 $j-1$，所以至多有$\left\lfloor \frac{j-1}{t} \right\rfloor$ 个 t 次不可约多项式 $g(z)$，使 $\mathbf{c}$ 不属于 $\Gamma(L,g)$．要保证距离 d，我们至多应该排除

$$\sum_{j=1}^{d-1} \left\lfloor \frac{j-1}{t} \right\rfloor (q-1)^j \binom{n}{j}$$

个 t 次不可约多项式，这个数小于 $\frac{d}{t} V_q(n, d-1)$（见 (5.1.4)）．由(1.1.19)，$\mathbf{F}_{q^m}$ 上 t 次不可约多项式的个数超过

$$\left(\frac{1}{t}\right) q^{mt}(1 - q^{-\frac{1}{2}mt+1}).$$

因此，所需的码 $\Gamma(L,g)$ 存在的一个充分条件是：

$$\frac{d}{t} V_q(n, d-1) < \frac{1}{t} q^{mt}(1 - q^{-\frac{1}{2}mt+1}). \tag{8.4.2}$$

根据定理 8.2.7，所得的码至少有 q^{n-mt} 个码字．在(8.4.2)两边取以 q 为底的对数，再除以 n．假定 n 是变量，且 $\frac{d}{n} \to \delta$，$n \to \infty$，利用引理 5.1.6 得

$$H_q(\delta) + o(1) < \frac{mt}{n} + o(1).$$

由于码 $\Gamma(L,g)$ 的信息率$\geq 1 - \frac{mt}{n}$，所以，我们可以找到一列多项

式 $g(z)$，使得对应的 Goppa 码的信息率趋向 $1-H_q(\delta)$. 这就是 Gilbert 界(5.1.9). □

§ 8.5 Goppa 码的译码

在 § 6.7 中我们提到过 Berlekamp 译解 BCH 码的方法，这一方法也可用来译 Goppa 码. 为了说明这一点，我们用与 § 6.7 中同样的方法来进行.

设 $(C_0, C_1, \cdots, C_{n-1})$ 是 $\Gamma(L, g)$ 中如(8.2.4)所定义的一个码字，假定我们收到 $(R_0, R_1, \cdots, R_{n-1})$. 用 $\mathbf{E}=(E_0, E_1, \cdots, E_{n-1})=\mathbf{R}-\mathbf{C}$ 记差错向量. 令 $M:=\{i \mid E_i \neq 0\}$，记 $t=\deg g(z)$ 并假定 $|M|=e<\frac{1}{2}t$. 再利用(8.2.3)的约定，定义一个多项式 $S(x)$：

$$(8.5.1) \qquad S(x) \equiv \sum_{i=0}^{n-1} \frac{E_i}{x-\gamma_i} \pmod{g(x)}.$$

$S(x)$ 称为**校验子**. $S(x)$ 可以由接收者利用 $\mathbf{R}$ 及(8.2.5)计算出来. 再用与 § 6.7 类似的方法定义一个**找差错位多项式** $\sigma(z)$ 和一个相伴多项式 $\omega(z)$(但这次是应用错位本身，而不是它们的逆).

$$(8.5.2) \qquad \sigma(z):=\prod_{i \in M}(z-\gamma_i),$$

$$(8.5.3) \qquad \omega(z):=\sum_{i \in M} E_i \prod_{j \in M \setminus \{i\}}(z-\gamma_j).$$

由定义，$\sigma(z)$ 与 $\omega(z)$ 无公因式，且 $\deg \sigma(z)=e$，$\deg \omega(z)<e$. § 6.7 中有关 $\omega(z)/\sigma(z)$ 的计算可用下式代替：

$$(8.5.4) \qquad S(z)\sigma(z) \equiv \sum_{i=0}^{n-1} \frac{E_i}{z-\gamma_i} \prod_{i \in M}(z-\gamma_i) \equiv \omega(z) \pmod{g(z)}.$$

现在假定我们已有一个算法，可找到一个次数最低的首一多项式 $\sigma_1(z) \neq 0$ 以及一个次数最低的多项式 $\omega_1(z)$，使得

$$(8.5.5)\qquad S(z)\sigma_1(z)\equiv\omega_1(z)\ (\mathrm{mod}\,g(z)).$$

若 $d(z)$ 是 $S(z)$ 和 $g(z)$ 的最大公因式，则由(8.5.4)与(8.5.5)知 $d(z)$ 整除 $\omega(z)$ 和 $\omega_1(z)$. 再由(8.5.4)和(8.5.5)得

$$\frac{S(z)}{d(z)}\left\{\frac{\omega_1(z)\sigma(z)-\omega(z)\sigma_1(z)}{d(z)}\right\}\equiv 0\ \left(\mathrm{mod}\,\frac{g(z)}{d(z)}\right).$$

由此就有

$$\omega_1(z)\sigma(z)-\omega(z)\sigma_1(z)\equiv 0\ (\mathrm{mod}\,g(z)).$$

因为上式左边的次数小于 $g(z)$ 的次数，所以应为 0. 而 $(\sigma(z),\omega(z))=1$ 意味着 $\sigma(z)$ 可整除 $\sigma_1(z)$，于是有 $\sigma_1(z)=\sigma(z)$. 一旦找到了 $\sigma(z)$ 与 $\omega(z)$，很明显，我们就找到了 **E**. Berlekamp 算法是计算 $\sigma_1(z)$ 的一个有效方法. 还有另一种基于 Euclid 算法的方法，可用来求两个多项式的最大公因式.

§8.6 广义 BCH 码

我们从别的方面来考察 Goppa 码. 令 $L=\{1,\beta,\beta^2,\cdots,\beta^{n-1}\}$，其中 β 是 $\mathbf{F}_{2^m}$ 中的 n 次本原单位根，取 $g(z)$ 为一适当的多项式. 设 $(a_0,a_1,\cdots,a_{n-1})\in\Gamma(L,g)$. 如(6.5.2)，我们用 $A(X)$ 记 $a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ 的 Mattson-Solomon 多项式.

考虑多项式

$$(X^n-1)\sum_{i=0}^{n-1}\frac{A(\beta^i)}{X-\beta^i}=(X^n-1)n\sum_{i=0}^{n-1}\frac{a_i}{X-\beta^i}$$

(这里用到引理 6.5.3).

上式左边是一个次数 $\leqslant n-1$ 的多项式，并且在 $X=\beta^i(0\leqslant i\leqslant n-1)$ 处取值 $n\beta^{-i}A(\beta^i)$. 由于我们只在 $\mathbf{F}_2$ 上讨论问题，所以 n 可以换成 1. 又因为 $X^{n-1}\circ A(X)$ (用 §6.5 中的记号)的次数 $\leqslant n-1$ 并且也在这 n 个 n 次单位根上取同样的值，所以上式左边就是多项式 $X^{n-1}\circ A(X)$. 这就证明了

(8.6.1)定理. 设 β 是 $\mathbf{F}_{2^m}$ 中的一个 n 次本原单位根. 若 $L=\{1,\beta,\beta^2,\cdots,\beta^{n-1}\}$，$(g(z),z^n-1)=1$，则二元 Goppa 码 $\Gamma(L,g)$

由所有使得 $a(x)$ 的 Mattson 多项式 $A(X)$ 满足

$$X^{n-1}\circ A(X)\equiv 0 \pmod{g(X)}$$

的字 $(a_0,a_1,\cdots,a_{n-1})$ 组成.

在定理 6.6.2 中，我们利用定理 6.5.5 以及码字的 Mattson-Solomon 多项式具有充分小的次数证明了 BCH 界. 对于 Goppa 码，我们有类似的结果. 现在多项式 $g(X)$ 的次数为 t，$(g(X), X^n-1)=1$，因此根据定理 8.6.1 可知 $A(X)$ 至少有 $n-1-t$ 个 n 次单位根为其零点. 因而又知 $\mathbf{a}$ 的重量至少为 $t+1$. 这是定理 8.2.7 的第二个证明.

以上结论告诉我们如何去推广这些码，其关键是要保证码字的 Mattson-Solomon 多项式的零点中所含 n 次单位根的个数极少,这一想法曾为 R. T. Chen 和 D. M. Choy (1975,[13]) 所采用.

(8.6.2)定义. 设 $\mathscr{F}=\mathbf{F}_{q^m}$，$(T,+,0)$ 的定义如 § 6.5，令 $S=\mathbf{F}_q[x]\bmod(x^n-1)$. 假定 $P(X)$ 和 $G(X)$ 是 T 中的两个多项式且 $(P(X), X^n-1)=(G(X), X^n-1)=1$. 那么,$\mathbf{F}_q$ 上由多项式对 $(P(X),G(X))$ 决定的,字长为 n 的广义 BCH 码(记作 GBCH) 定义为

$$\{a(x)\in S\,|\,P(X)\circ(\Phi a)(X)\equiv 0(\bmod G(X))\}.$$

显然,GBCH 码是线性码.

(8.6.3)定理. 由 (8.6.2) 定义的 GBCH 码的极小距离 $\geqslant 1+\deg G(X)$.

证明. 由定理 6.5.5,Φa 与 X^n-1 的公因式 $f(X)$ 也是 $P(X)\circ(\Phi a)(X)$ 的因式,但 $(G(X),f(X))=1$,所以 $f(X)$ 的次数至多是 $n-1-\deg G(X)$. □

注意，定理 8.6.1 中特殊的 Goppa 码就是 GBCH 码的例子. 若取 $P(X)=X^{n-1}$,$G(X)=X^{d-1}$,则又得到一个 BCH 码.

GBCH 码的奇偶校验矩阵类似于 § 8.1 中的 $\hat{H}$. 为证此，考虑多项式 $p(x)=(\Phi^{-1}P)(x)=\sum_{i=0}^{n-1}p_ix^i$ 和 $g(x)=(\Phi^{-1}G)(x)=$

$\sum_{i=0}^{n-1} g_i x^i$. 因为 n 次单位根不是 $P(X)$ 与 $G(X)$ 的零点，所以根据引理 6.5.3 知 $p(x), g(x)$ 的所有系数都是非零的. 设 $a(x)$ 是一个码字，$A(X) = (\Phi a)(X)$. 由(8.6.2)知，有一个次数不超过 $n-1-\deg G(X)$ 的多项式 $B(X)$ 使

$$P(X) \circ A(X) = B(x)G(x) = B(X) \circ G(X).$$

令 $b(x) := (\Phi^{-1}B)(x) = \sum_{i=0}^{n-1} b_i x^i$,那么我们有

$$p(x) * a(x) \doteq b(x) * g(x),$$

即

$$\sum_{i=0}^{n-1} p_i a_i x^i = \sum_{i=0}^{n-1} b_i g_i x^i.$$

于是,$b_i = p_i g_i^{-1} a_i$ $(0 \leqslant i \leqslant n-1)$. 再令 $h_i := p_i g_i^{-1}$,定义

$$H := \begin{bmatrix} h_0 & h_1\beta & \cdots & h_{n-1}\beta^{n-1} \\ h_0 & h_1\beta^2 & \cdots & h_{n-1}\beta^{2(n-1)} \\ \cdots & \cdots & \cdots & \cdots \\ n_0 & h_1\beta^t & \cdots & h_{n-1}\beta^{t(n-1)} \end{bmatrix}.$$

设 $1 \leqslant j \leqslant t = \deg G(X)$,则 $B_{n-j} = 0$. 由(6.5.2),

$$B_{n-j} = b(\beta^j) = \sum_{i=0}^{n-1} b_i \beta^{ij} = \sum_{i=0}^{n-1} h_i a_i \beta^{ij},$$

所以有 $\mathbf{a}H^T = \mathbf{0}$. 反之，若 $\mathbf{a}H^T = \mathbf{0}$, 则 $B(X)$ 的次数至多为 $n-1-t$,所以 $B(X)G(X) = B(X) \circ G(X) = P(X) \circ A(X)$, 即 $\mathbf{a}$ 属于这个 GBCH 码.

§8.7 评　　注

§8.1 中所描述的码叫做交错码. 本章所涉及的码是依赖于 h_i 和 β_i 的选择的特殊情况. 最有趣的子类似乎要算由 J.N. Srivastava 于 1967 年所引进的 Srivastava 码了(未发表). E. R. Berlekamp ([2]) 认识到了它们的可能性并建议在这方面作进一步的

研究。交错码是 H. J. Helgent (1974;[35]) 所引入的，由 V. D. Goppa ([27]) 在 1970 年引进的 Goppa 码是其中最有趣的例子(见[4])。

除了 E. R. Berlekamp 与 O. Moreno ([5]) 所证明的扩张 2-纠错二元 Goppa 码是循环码以外，BCH 码是仅有的循环 Goppa 码（见问题 8.8.2)。后来，K. K. Tzeng 和 K. P. Zimmerman ([71]) 对其它的 Goppa 码也证明了类似的结果，并且推广了 Goppa 码的思想。

§8.8 问 题

8.8.1. 设 L 由 $\mathbb{F}_{2^4}$ 中的所有 15 次本原单位根组成（取 $\alpha^4+\alpha+1=0$)。令 $g(z):=z^2+1$. 试剖析二元 Goppa 码 $\Gamma(L,g)$.

8.8.2. 设 α 是 $\mathbb{F}_{2^m}$ 中的一个 n 次本原单位根，令 $L:=\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$. 证明当二元 Goppa 码 $C=\Gamma(L,g)$ 为循环码时，必有某 t 使 $g(z)=z^t$，即 C 为 BCH 码。

8.8.3. 设 $n=q^m-1$, $L=\mathbb{F}_{q^m}\backslash\{0\}$. 再设 C_1 是于(6.6.1)中取 $l=0$, $\delta=d_1$ 得到的 $\mathbb{F}_q$ 上长为 n 的 BCH 码，而 C_2 是 Goppa 码 $\Gamma(L,g)$. 证明 $C_1\cap C_2$ 的极小距离 $d\geqslant d_1+d_2-1$.

8.8.4. 考虑多项式对 $(P(X), G(X))$ 所确定的 GBCH 码，其中 $\deg G(X)=t$. 证明存在多项式 $\hat{P}(X)$，使 $(\hat{P}(X),X^t)$ 确定同一个码。

8.8.5. 设 C 是长为 15 的二元循环码，生成多项式为 x^2+x+1. 证明 C 是 BCH 码但不是 Goppa 码。

第九章　渐近代数优码

§ 9.1　一个简单的非构造性例子

在前面各章中，我们叙述了几种构造码的方法。如果用第五章的观点来考察这些码，我们可能会感到失望。§ 4.1 中的 Hadamard 码具有 $\delta=\frac{1}{2}$，但当 $n\to\infty$ 时，它们的信息率 R 趋于 0。对于 Hamming 码，虽然 R 趋于 1 但 δ 趋于 0。对于 BCH 码，若固定 R，则也有 $\delta\to 0$。对所有我们讨论过的码，都有一个确定的码序列存在，使得 $\delta\to 0$ 或者 $R\to 0$。

作为下节的引言，我们现在证明可以给出一个产生优码的简单的代数定义。然而，这个定义不是构造性的，并且仍停留在定理 2.2.3 所阐述的观点上。我们将讨论 $R=\frac{1}{2}$ 的二元码。固定一个 m 并选择元 $\alpha_m\in\mathbf{F}_{2^m}$。如何选择这个元素将在下面给以解释。把向量 $\mathbf{a}\in\mathbf{F}_2^m$ 看作 $\mathbf{F}_{2^m}$ 中的元，定义

$$C_\alpha:=\{(\mathbf{a},\alpha\mathbf{a})\mid\mathbf{a}\in\mathbf{F}_2^m\}.$$

设 $\lambda=\lambda_m$ 已给定。若 C_α 包含一个重量 $<2m\lambda$ 的非零字 $(\mathbf{a},\alpha\mathbf{a})$，则 α 作为 $\alpha\mathbf{a}$ 与 $\mathbf{a}$ 的商(在 $\mathbf{F}_{2^m}$ 中)由这个字所唯一确定。由此可见，α 至多有 $\sum_{i<2m\lambda}\binom{2m}{i}$ 种选择使导出的码 C_α 的极小距离 $<2m\lambda$。现在取 $\lambda=H^{\leftarrow}\left(\frac{1}{2}-(1/\log m)\right)$。根据定理 1.4.5，$\alpha$ 的“不良”选择的数目是 $o(2^m)(m\to\infty)$。所以，几乎对 α 的所有选择都有

$$d\geqslant 2mH^{\leftarrow}\left(\frac{1}{2}-\frac{1}{\log m}\right),$$

其中 d 是 C_α 的极小距离，令 $m\to\infty$ 并适当选取 α_m，我们得到一个信息率均为 $\frac{1}{2}$ 的码序列且使得对应的 δ 满足

$$\delta = H^{\leftarrow}\left(\frac{1}{2}\right) + o(1),\ (m\to\infty).$$

因此，这个序列满足 Gilbert 界 (5.1.9). 如果我们能够给出一个选取 α_m 的明确方法，那将是一个惊人的结果．长期以来，都存在这样一系列的疑问，是否有可能给出一个确定码序列的明确的代数方法，使得信息率与 d/n 都界于 0 之外？Justesen（[37]）于 1972 年成功地做到了这一点，其基本思想是上述方法的一种变形，在一个码字中让所有可能的乘数 α 都出现，用以代替这里难以选取的 α 值，而这多个乘数 α 的平均效果几乎与单个 α 的某种明智选择同样好。

§9.2 Justesen 码

我们将要研究的码是 G. D. Forney（[22]）在 1966 年引入的级联码的一种推广． 级联码的基本想法是分两步来构造一个码：从一个码 C_1 出发，把 C_1 中的码字看作一个新字母集中的符号，而码 C_2 是由这些符号构造出来的．对此，我们将予以详细讨论． 设 C_2 是 $\mathbf{F}_{2^m}$ 上的一个码，码字 $(c_0,c_1,\cdots,c_{n-1})$ 中的符号 c_i 可以写成 $\mathbf{F}_2$ 上的一个 m-元组，即 $c_i=(c_{i1},c_{i2},\cdots,c_{im})$ $(i=0,1,\cdots,n-1)$，其中 $c_{ij}\in\mathbf{F}_2$．对于所谓的内部码 C_1 中的一个码字来说，这样的一个 m-元组就是它的信息符号序列．我们只考虑码率为 $\frac{1}{2}$ 的最简情况．对应于 $c_i=(c_{i1},c_{i2},\cdots,c_{im})$，在内部码中有一个长为 $2m$ 的字．

级联码的码率是 C_2 的码率的一半．Justesen 的想法是使内部码 C_1 为可变的，即 C_1 的选择取决于 i． 如上节所述，选择内部码使得一个长为 $2m$ 的字起始于 c_i 的符号序列． 我们再取一个 Reed-Solomon 码作为外部码 C_2.

构造的细节如下．由于我们打算令m趋于无穷，所以需要有结构简单的 $\mathbf{F}_{2^m}$． 利用定理 1.1.28，取 $m = 2 \cdot 3^{l-1}$ 并把 $\mathbf{F}_{2^m}$ 用 $\mathbf{F}_2[x](\bmod g(x))$ 表示，这里 $g(x) = x^m + x^{m/2} + 1$．作为外部码的 Reed-Solomon 码（见 § 6.8）C_2 如下表示． 将 m-元组 $(i_0, i_1, \cdots, i_{m-1})$ 看作 $\mathbf{F}_{2^m}$ 中的元素 $i_0 + i_1x + \cdots + i_{m-1}x^{m-1}$． 取 K个连续的 m-元组 $a_0, a_1, \cdots, a_{k-1}$，构造多项式 $a(Z) := a_0 + a_1Z + \cdots + a_{k-1}Z^{k-1} \in \mathbf{F}_{2^m}[Z]$．对于 $j = 1, 2, \cdots, N := 2^m - 1$，定义 $j(x) = \sum_{i=0}^{m-1} \varepsilon_i x^i$，如果 j 的二进制表示为 $\sum_{i=0}^{m-1} \varepsilon_i 2^i$． 这样 $j(x)$ 取遍了 $\mathbf{F}_{2^m}$ 中的所有非零元．将它们分别代入 $a(Z)$，得到一个含 $\mathbf{F}_{2^m}$ 中N个元的序列，它就是线性码 C_2 中的一个码字． C_2 的码率为 K/N．由于 $a(Z)$ 的次数 $\leqslant K-1$，所以它至多有 $K-1$ 个零点，即 C_2 的极小重量 $D \geqslant N - K + 1$（见 §6.8）． 这是产生 Reed-Solomon 码序列的一个完整的方法． 我们以同样的方法来构造内部码． 若 c_j 是外部码中一个码字的第 i 个符号(仍表为 $\mathbf{F}_2$ 上的多项式)，则把它换成$(c_j, j(x)c_j)$，这里乘法取 $\bmod g(x)$．最后，把它们表成 $\mathbf{F}_2$ 上的 $2m$-元组．

(9.2.1)定义． 设 $m = 2 \cdot 3^{l-1}$，$N = 2^m - 1$，适当选择 K（见下面），并令 $D = N + 1 - K$．以 $\mathscr{C}_m$ 记如上定义的长为 $n := n_m := 2mN$ 的二元码，称之为 Justesen 码． $\mathscr{C}_m$ 的维数为 $k := mK$，码率为 $K/2N$．

我们采用与 § 9.1 中类似的想法来分析 $\mathscr{C}_m$，就是说，出现在 $\mathscr{C}_m$ 的一个码字中的非零 $2m$-元组 $(c_j, j(x)c_j)$ 确定了 i 的值．

(9.2.2)引理． 设 $\gamma \in (0,1)$，$\delta \in (0,1)$．又设 $(M_L)_{L \in \mathbf{N}}$ 是一个自然数列具有性质 $M_L \cdot 2^{-L\delta} = \gamma + o(1)(L \to \infty)$．用$W$记 $\mathbf{F}_2^L$ 中 M_L 个不同字的重量和，那么

$$W \geqslant \gamma L 2^{L\delta}\{H^{\leftarrow}(\delta) + o(1)\}, \quad (L \to \infty).$$

证明． 对充分大的 L 定义

$$\lambda := H^{\leftarrow}\left(\delta - \frac{1}{\log L}\right).$$

由定理 1.4.5 有

$$\sum_{0\leqslant i\leqslant\lambda L}\binom{L}{i}\leqslant 2^{L(\delta-(1/\log L))}.$$

所以

$$W\geqslant\left\{M_L-\sum_{0\leqslant i\leqslant\lambda L}\binom{L}{i}\right\}\lambda L\geqslant\lambda L\{M_L-2^{L(\delta-(1/\log L))}\}$$

$$=\lambda L2^{L\delta}\{\gamma+o(1)\}=\gamma L2^{L\delta}\{H^{\leftarrow}(\delta)+o(1)\},$$

$$(L\to\infty).$$ □

选择码率 R 使 $0<R<\frac{1}{2}$. 取(9.2.1)的数 K 为使 $R_m:=K/2N\geqslant R$ 成立的最小值. 这保证了在(9.2.1)中取 $l=1,2,\cdots$得到的码序列 $\mathscr{C}_m$ 具有码率 $R_m\to R(l\to\infty)$. $\mathscr{C}_m$ 的极小距离又怎样呢? 在外部码中,一个非零码字的重量至少为 $N-K+1=D$. 进一步有

(9.2.3) $$N-K+1>N-K=N(1-2R_m)$$
$$\doteq(2^m-1)\{1-2R+o(1)\},(m\to\infty).$$

外部码的一个码字中的每个非零符号在 $\mathscr{C}_m$ 的一个对应的码字 $\mathbf{c}$ 中产生一个 $2m$-元组 $(c_j, j(x)c_j)$, 并且它们都不相同 (根据(9.2.1)后的附注). 我们用引理 9.2.2 来估计 $\mathbf{c}$ 的重量. 取 $L=2m$, $\delta=\frac{1}{2}$,$\gamma=1-2R$, $M_L=D$. 由(9.2.3),引理的条件已满足,所以

$$w(\mathbf{c})\geqslant(1-2R)\cdot 2m\cdot 2^m\cdot\left\{H^{\leftarrow}\left(\frac{1}{2}\right)+o(1)\right\},\ (m\to\infty).$$

于是有

$$\frac{d_m}{n}\geqslant(1-2R)\left\{H^{\leftarrow}\left(\frac{1}{2}\right)+o(1)\right\},\ (m\to\infty).$$

由此,我们证明了下列定理.

(9.2.4)定理. 设 $0<R<\frac{1}{2}$. 如上定义的 Justesen 码 $\mathscr{C}_m$ 具有字

长 $n = 2m(2^m - 1)$，信息率 R_m 以及极小距离 d_m，其中

(i) $R_m \to R, (m \to \infty)$,

(ii) $\liminf\limits_{n\to\infty} \frac{d_m}{n} \geqslant (1-2R)H^{\leftarrow}\left(\frac{1}{2}\right)$.

用第五章的记号，对于小于 $\frac{1}{2}$ 的 R，我们有

$$\delta \geqslant (1 - 2R)H^{\leftarrow}\left(\frac{1}{2}\right),$$

因此 δ 不趋于 $0 (n \to \infty)$.

为了使信息率大于 $\frac{1}{2}$，必须将前面所述稍加改变．设 $0 \leqslant s < m$ (后面将选择 s)，考虑 $\mathscr{C}_m$．对于码字 $\mathbf{c}$ 中的每一个 $2m$-元组 $(c_j, j(x)c_j)$，我们去掉最后 s 个符号，导出的码记作 $\mathscr{C}_{m,s}$． 令 R 固定，$0 < R < 1$．给定 m 和 s，选取使得 $R_{m,s} := [m/(2m-s)] \times (K/N) \geqslant R$ 的最小整数 K (若 $m/(2m-s) \geqslant R$，这是可能的)．在定理 9.2.4 的证明中，用到了码字 $\mathbf{c}$ 至少包含有 D 个不同的 $2m$-元组 $(c_j, j(x)c_j)$ 这一事实．由于码字缩短了，我们得到的 $(2m-s)$-元组不一定互不相同，但每个可能的值至多只出现 2^s 次．因此在 $\mathscr{C}_{m,s}$ 的码字 $\mathbf{c}$ 中，至少有

$$M_s := 2^{-s}(N - K) = 2^{-s}N\left(1 - \frac{2m-s}{m}R_{m,s}\right)$$

个不同的 $(2m-s)$-元组．

再次应用引理 9.2.2，这时

$$L = 2m - s, \delta = \frac{m-s}{L}, \gamma = 1 - \frac{2m-s}{m}R,$$

$$M_L = M_s.$$

令 $d_{m,s}$ 是 $\mathscr{C}_{m,s}$ 的极小距离，我们有

$$d_{m,s} \geqslant \left(1 - \frac{2m-s}{m}R\right)(2m-s)2^{m-s}\left\{H^{\leftarrow}\left(\frac{m-s}{2m-s}\right) + o(1)\right\}2^s, (m \to \infty).$$

所以

$$(9.2.5)\quad \frac{d_{m,s}}{n} \geqslant \left(1-\frac{2m-s}{m}R\right)\left\{H^{\leftarrow}\left(\frac{m-s}{2m-s}\right)+o(1)\right\},$$

$$(m\to\infty).$$

现在要寻找 s 的某种选择，使产生的结果最佳. 令 r 固定，$r\in\left(\frac{1}{2},1\right)$. 取 $s:=\lfloor m(2r-1)/r\rfloor+1$. 若 $r\geqslant R$,则 $m/(2m-s)\geqslant R$. 由(9.2.5)有

$$(9.2.6)\quad \frac{d_{m,s}}{n} \geqslant \left(1-\frac{R}{r}\right)\{H^{\leftarrow}(1-r)+o(1)\},(m\to\infty).$$

若 r 满足

$$(9.2.7)\qquad R=\frac{r^2}{1+\log\{1-H^{\leftarrow}(1-r)\}},$$

则(9.2.6)右边达到最大值. 如果(9.2.7)的解小于 $\frac{1}{2}$,则取 $r=\frac{1}{2}$.

下面的定理是对这一构造方法的总结.

(9.2.8)定理. 设 $0<R<1$,r 是 $\frac{1}{2}$ 与(9.2.7)的解中之最大者. 令 $s=\lfloor m(2r-1)/r\rfloor+1$, 那么 Justesen 码 $\mathscr{C}_{m,s}$ 具有字长 n, 信息率 $R_{m,s}$, 极小距离 $d_{m,s}$ 其中

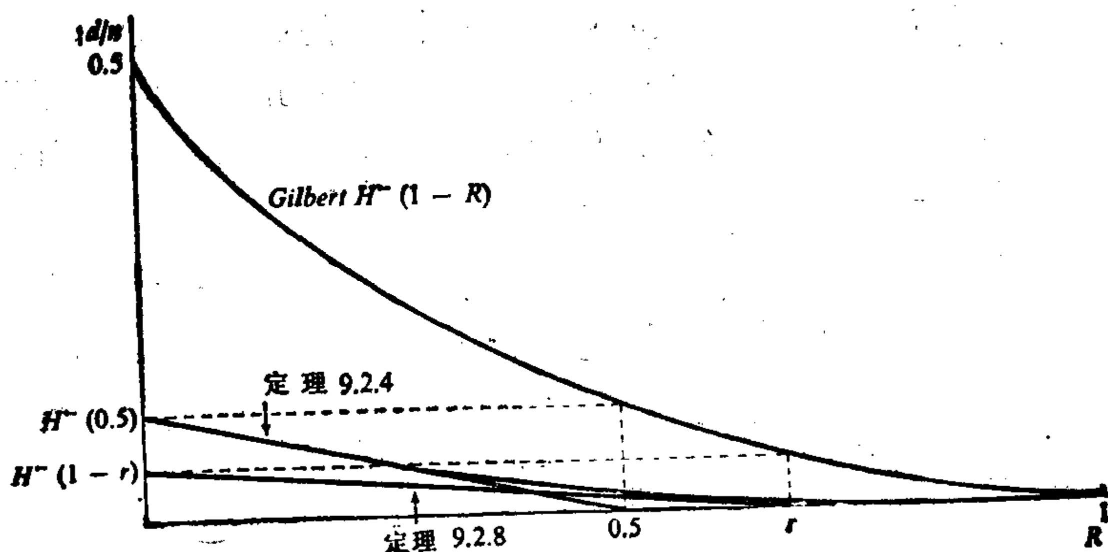


图 3

$$\liminf \frac{d_{m,s}}{n} \geqslant \left(1 - \frac{R}{r}\right) H^{\leftarrow}(1 - r).$$

在图 3 中，我们把 Justesen 码与 Gilbert 界作了对比。对 $r > \frac{1}{2}$，曲线是(9.2.6)所给线族的包络。

§ 9.3 评　注

§ 9.1 中的极其简单的想法至今尚未引起足够的重视．更多的尝试可能会发现 α 的明确选取方法，使之产生相当好的码(除问题 9.4.1 所述外)。 Justesen 码的发现是七十年代编码理论的重大进展之一。

§ 9.4 问　题

9.4.1. 设 $\mathbf{F}_{2^6}$ 如 § 9.2 所表示．证明不存在这样的 α，使得按 § 9.1 构造出的 C_α 的距离大于 3．比较其它已知的，码率 $\geqslant \frac{1}{2}$ 的 $[12, k]$ 码．

9.4.2. 设 $\alpha(x)$ 是一次数小于 k 的多项式．一个二元 $[2k, k]$ 双循环码是由所有形如 $(a(x), \alpha(x)a(x))$ 的码字组成的，其中乘法取 $\bmod(x^k - 1)$．这时，若对码字的两半同时作循环平移变换，则码不变．试构造一个这种类型的 $[12, 6]$ 码，使 $d = 4$．

9.4.3. 用 § 9.2 中的缩减方法证明：对任意码率 R，按 § 9.2 中想法导出的码都满足 Gilbert 界．

第十章 算 术 码

§ 10.1 AN 码

在这一章中，我们扼要地介绍一种用于检查和改正计算机运算错误的码. 这里，运算是指通常的算术运算，因而其理论与前述各章完全不同. 然而在几个地方与循环码的理论有相似之处. 在某些情况下，我们将证明的细节留给读者. 关于这一领域更一步的讨论，请读者阅读 § 10.4 所给出的文献.

这一章中，进行运算的数，是在以基数 $r(r\in \mathrm{N},\ r\geqslant 2)$ 的数系中表出的. 从实际应用的角度看，2-进制 ($r=2$) 和 10-进制 ($r=10$) 的情形是最重要的. 我们必须做的第一件事，是寻找一个适当的距离函数. 前述各章曾使用过的 Hamming 距离并不适合目前的讨论. 这是因为做加法时产生的一个差错，会因进位而导致运单结果的许多位发生差错. 我们需要的距离函数，它对应于算术差错就象 Hamming 距离对应于字符印刷错误一样.

(10.1.1)定义. 一个整数 x 的**算术重量** $w(x)$，是使存在下述表示的最小的 t

$$x=\sum_{i=1}^{t} a_i r^{n(i)},$$

这里 $a_i, n(i)$ 是整数，且 $|a_i|<r, n(i)\geqslant 0 (i=1,2,\cdots,t)$. 两个整数之间的**算术距离** $d(x,y)$ 定义为

$$d(x,y):=w(x-y).$$

容易验证，这的确是 $\mathbf{Z}$ 的一个度量. 算术距离是平移不变的，即 $d(x,y)=d(x+z,y+z)$. 然而对于(表成 r-进制的)两个整数的 Hamming 距离而言，这并不成立. 算术距离不超过 Hamming 距离.

我们将要讨论具有如下形式的码 C:

$$C := \{\mathrm{AN} \mid N \in \mathbf{Z},\ 0 \leqslant N < B\},$$

其中,A 和 B 都是固定的正整数. 这样的码称为 AN 码. 这些码有如下的应用. 假定我们希望求出两个整数 N_1, N_2(正的且小于 B)的和,那么我们先把它们编码成 AN_1 和 AN_2,然后将这两个整数相加,设和为 S. 如果运算正确,则用 A 除 S 就可得到 $N_1 + N_2$. 如果 A 不能除尽 S,就说明出现了错误. 这时寻找码字 AN_3,使 $d(S, AN_3)$ 达到最小,那么 N_3 就是 $N_1 + N_2$ 的极大似然值. 为了能够纠正所有可能的至多含 e 个差错的模式,充分必要条件仍然是码 C 的极小距离 $\geqslant 2e+1$. 如前,这等价于要求码 C 的极小重量至少为 $2e+1$. 码 C 的这些性质,基于它与 $\mathbf{Z}$ 的子群 $H := \{AN \mid N \in \mathbf{Z}\}$ 的相似性. 由于 H 的极小重量 $\leqslant 2$ (见问题 10.5.1),因此把 H 取做我们所要的码并不是一个好主意.

为了避开这个难点,我们考虑所谓的**模 AN 码**. 定义 $m := AB$,则我们可以把 C 看做 $\mathbf{Z}/m\mathbf{Z}$ 的子群. 因此,有必要修改我们的距离函数. 视 $\mathbf{Z}/m\mathbf{Z}$ 的元素为图 Γ_m 的顶点,这里 $x(\mathrm{mod}\,m)$ 与 $x'(\mathrm{mod}\,m)$ 有边相连当且仅当

$$x - x' \equiv \pm c r^i \pmod m$$

对某两个整数 $c, i, 0 < c < r,\ i \geqslant 0$.

(10.1.2)定义. 两个整数 x 和 y (看作 $\mathbf{Z}/m\mathbf{Z}$ 的元素)的**模距离** $d_m(x,y)$ 是 x 和 y 在图 Γ_m 中的距离. x 的**模重量** $w_m(x)$ 定义为 $d_m(x, 0)$. 注意

$$w_m(x) = \min\{w(y) \mid y \in \mathbf{Z},\ y \equiv x(\mathrm{mod}\,m)\}.$$

尽管我们已经得到了与线性码的一个极强的相似,然而还有别的困难. 并非 m 的任何选择都有良好意义. 例如,当我们取 $r = 3, A = 5, B = 7$ 时,$m = 35$. 由于 $4 \equiv 3^{10}(\mathrm{mod}\,35)$,我们有 $d_m(0, 4) = 1$. 但是,当参与加法运算的整数比 35 小时,考虑对应于 3^{10} 这一位置的差错就不太切合实际了. 而在 Γ_m 的定义中,限制 i 也有不足之处. 事实证明,如果取 $m = r^n - 1(n \in \mathbf{Z}, n \geqslant 2)$,就能够得到可以接受的理论. 在实际应用中,这也是一个很好的

选择，因为许多计算机都是模 2^n-1 进行运算的。

每个整数 x 都可唯一地表示为

$$x\equiv\sum_{i=0}^{n-1}c_i n^i(\bmod r^n-1),$$

这里 $c_i\in\{0,1,\cdots,r-1\}$ $(0\leqslant i<n)$，c_i 不全为 0. 因此 $\mathbf{Z}/(r^n-1)$ 可以看作是字母集 $\{0,1,\cdots,r-1\}$ 上的长为 n 的非零字所成的集合. 当然，如果我们取 $m=r^n$，就没有必要将 0 排除在外了. 注意到许多计算机是模 2^n 工作的，所以 $m=r^n$ 也是一种有实际意义的选择. 但在 $r=2$, $m=2^n$ 时，我们却不能指望得到好码. 因为我们必须取 $A=2^k$（对某个 k），从而码 C 将由形如 $\sum_{i=0}^{n-1}c_i2^i$, $c_i\in\{0,1\}$, $c_0=\cdots=c_{p-1}=0$ 的整数所组成，这时，对一个整数 $x(\bmod B)$ 进行编码，就是在它的表示里加上 k 个 0. 这是毫无意义的，对任意的 r 都存在类似的问题. 读者应该确信，在 $AB=m=r^n-1$ 的情形，模距离对于 $\mathbf{Z}/m\mathbf{Z}$ 的算术运算是一个自然的函数，因而 C 很象线性码. 事实上，我们可以得到与前述各章更强的相似.

(10.1.3)定义. 一个以 r 为底的长为 n 的循环 AN 码是 $\mathbf{Z}/(r^n-1)$ 的一个子群 C. 它是这个环中的主理想，即存在 A, B, 使 $AB=r^n-1$，并且

$$C=\{AN|N\in\mathbf{Z},0\leqslant N<B\}.$$

象 § 6.1 那样，我们称 A 为 C 的生成元. 至此，读者就不会奇怪我们的主要兴趣在于那些具有较大信息率 $\left(=\frac{1}{n}\log_r B\right)$ 和较大极小距离的码 C 了. 定义(10.1.3)中的术语与(6.1.1)是一致的. 如果 $x\in C$，则因为 C 是一个子群，所以 $rx(\bmod r^n-1)$ 也是 C 的一个码字，并且 $rx(\bmod r^n-1)$ 的确是 x 的一个循环移位（均以 r 为底表示）. 整数 B 好比是一个循环码的校验多项式.

用同样的方法，可以推广负循环码的思想. 这只须取 $m=r^n+1$，并考虑 $\mathbf{Z}/m\mathbf{Z}$ 的子群即可。

(10.1.4)例. 设 $r=2, n=11$, 则 $m=r^n-1=2047$. 我们取 $A=28$, $B=89$. 得到的循环 AN 码由 23 的直到 2047 的全部 89 个倍数组成的. 一共有 22 种方式产生一个差错，这些差错对应于整数 $\pm 2^j (0 \leqslant j < 11)$. 它们恰好是除 0 之外的模 23 剩余. 因此, $[1, 2047]$ 中的每个整数恰与一个码字的模距离为 0 或 1. 所以, 这个循环码是**完全的**. 它是 Hamming 码的推广.

§ 10.2 算术重量和模重量

为了能构造出可纠正多于一个差错的 AN 码，我们需要一个简单的方法来计算整数的算术重量和模重量.

由定义 10.1.1, 每个整数 x 都可以表示为

$$x=\sum_{i=1}^{w(x)} a_i r^{n(i)}$$

其中 $a_i, n(i)$ 是整数, $|a_i|<r$, $n(i) \geqslant 0 (i=1,2,\cdots, w(x))$. 容易找到例子说明这种表示不是唯一的. 为此，我们要对系数再加一些限制, 以使这种表示成为唯一的.

(10.2.1)定义. 设 $b \in \mathbf{Z}, c \in \mathbf{Z}, |b|<r, |c|<r$. 偶 (a, b) 称为**容许的**, 如果下述条件之一成立:

(i) $bc=0$,

(ii) $bc>0$ 并且 $|b+c|<r$,

(iii) $bc<0$ 并且 $|b|>|c|$.

注意, 若 $r=2$, 则必有可能性 (i). 因此, 如果一个表示

$$x=\sum_{i=0}^{\infty} c_i 2^i$$

内的所有的偶 (c_{i+1}, c_i) 都是容许的，那么必定没有两个相邻的非零系数. 这引出了**非邻接形式**(NAF) 这一名称. 现在, 我给们出它的更一般性的定义.

(10.2.2)定义. 设有一个表示

$$x=\sum_{i=0}^{\infty}c_ir^i,$$

其中 $c_i\in\mathbf{Z}, |c_i|<r$ 对一切 i,并且 $c_i=0$,对所有充分大的 i. 称这个表示为 x 的一个 NAF,如果对每个 $i\geqslant 0$, (c_{i+1}, c_i) 都是容许的.

(10.2.3)定理. 每个整数 x 都恰有一个 NAF. 如果

$$x=\sum_{i=0}^{\infty}c_ir^i$$

是 x 的 NAF,则

$$w(x)=|\{i|i\geqslant 0,\ c_i\neq 0\}|.$$

证明.

(a) 设将 x 表示为 $\sum\limits_{i=0}^{\infty}b_ir^i, |b_i|<r$. 又设 i 是使 (b_{i+1},b_i) 非容许的最小值. 不失一般性,设 $b_i>0$ (否则考虑 $-x$). 用 $b'_i:=b_i-r$ 代替 b_i,用 $b'_{i+1}:=b_{i+1}+1$ 代替 b_{i+1}(若 $b_{i+1}+1=r$,则进位). 若 $b_{i+1}>0$,则 $b'_{i+1}=0$ 或者 $b'_ib'_{i+1}<0$,并且由于 (b_{i+1},b_i) 非容许而有 $b'_{i+1}=b_{i+1}+1>r-b_i=|b'_i|$. 若 $b_{i+1}<0$,则 $b'_{i+1}=0$ 或者 $b'_ib'_{i+1}>0$,并且因为 (b_{i+1}, b_i) 非容许而有 $-b_{i+1}<b_i$,因此,$|b'_i+b'_{i+1}|=r-b_i-b_{i+1}<r$,从而$(b'_{i+1},b'_i)$ 是容许的. 并且同理可以验证 (b'_i,b_{i-1}) 也是容许的. 按照这种方法,我们就可以构造一个 NAF,并且在这一过程中,表示的重量没有增加.

(b) 下面证明 NAF 是唯一的. 假设某个 x 有两个这样的表示: $x=\sum\limits_{i=0}^{\infty}c_ir^i=\sum\limits_{i=0}^{\infty}c'_ir^i$. 不失一般性,可以设 $c_0\neq c'_0$, $c_0>0$,因此 $c'_0=c_0-r$. 这意味着 $c'_1\in\{c_1+1-r, c_1+1, c_1+1+r\}$. 如果 $c'_1=c_1+1-r$,则 $c_1\geqslant 0$,因此有 $c_0+c_1\leqslant r-1$. 由 $c'_0c'_1>0$,必有$-c'_0-c'_1<r$, 即 $r-c_0+r-c_1-1<r$,所以 $c_0+c_1>r-1$. 矛盾. 同理假设 $c'_1=c_1+1$ 或 $c'_1=c_1+1+r$ 亦导出矛盾. 因此,NAF 是唯一的. □

下述定理提供了一个求NAF的直接方法。

(10.2.4)定理. 设 $x\in\mathbb{Z}, x\geqslant 0$. 设 $(r+1)x$ 和 x 的 r-元表示分别是

$$(r+1)x=\sum_{j=0}^{\infty}a_jr^j,\ x=\sum_{j=0}^{\infty}b_jr^j,$$

其中 $a_j,b_j\in\{0,1,\cdots,r-1\}$, 对所有的 j; 且 $a_j=b_j=0$, 对充分大的 j, 则 x 的 NAF 是

$$x=\sum_{j=0}^{\infty}(a_{j+1}-b_{j+1})r^j.$$

证明. 我们通过将 $\sum_{j=0}^{\infty}b_jr^j$ 与 $\sum_{j=0}^{\infty}b_jr^{j+1}$ 相加来计算 a_j. 设进位序列是 $\varepsilon_0,\varepsilon_1,\cdots$,则 $\varepsilon_0=0$, $\varepsilon_i:=\lfloor(\varepsilon_{i-1}+b_{i-1}+b_i)/r\rfloor$. 我们得到: $a_i=\varepsilon_{i-1}+b_{i-1}+b_i-\varepsilon_ir$. 记 $c_i:=a_i-b_i$, 则 $c_i=\varepsilon_{i-1}+b_{i-1}-\varepsilon_ir$. 我们必须验证 (c_{i+1}, c_i) 是容许的. $|c_{i+1}+c_i|<r$ 是 ε_i 的定义的平凡推论. 假设 $c_i>0$, $c_{i+1}<0$, 则 $\varepsilon_i=0$. 这时有 $c_i=\varepsilon_{i-1}+b_{i-1},c_{i+1}=b_i-r$, 同时条件 $|c_{i+1}|>|c_i|$ 等价于 $c_{i-1}+b_{i-1}+b_i<r$,即 $\varepsilon_i=0$. 最后一种情况是完全类似的. □

x 的 NAF 为我们提供了关于 x 的一个简单估计，详见下述定理.

(10.2.5)定理. 若我们用 $i(x)$ 代表 x 的 NAF 中使 $c_i\neq 0$ 的最大的 i,并且定义 $i(0):=-1$,则

$$i(x)\leqslant k\Longleftrightarrow|x|<\frac{r^{k+2}}{r+1}.$$

我们将这个完全初等的证明留给读者.

由 § 10.1,显然必须把这些思想用某种方式推广到模表示. 我们取 $m=r^n-1,n\geqslant 2$.

(10.2.6)定义. 一个表示

$$x\equiv\sum_{i=0}^{n-1}c_ir^i\pmod{m}\quad c_i\in\mathbb{Z},\ |c_i|<r,$$

称为 x 的一个 CNAF(＝循环 NAF)，如果 (c_{i+1}, c_i) 是容许的，对 $i=0,\cdots,n-1$。这里 $c_n:=c_0$。

下面的两个关于 CNAF 的定理，是定理 10.2.3 的直接推广。它们可由该定理得到，也可利用定理 10.2.5 推出。由于有意外，稍加小心是必要的。但是证明这些定理读者当无困难。

(10.2.7)定理. 每个整数 x 都有一个模 m CNAF，并且这个 CNAF 还是唯一的，除非

$$(r+1)x \equiv 0 \not\equiv x \pmod{m},$$

在这种情况下，x 有两个模 m CNAF。如果 $x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{m}$ 是 x 的 CNAF，则

$$w_m(x) = |\{i \mid 0 \leqslant i < n,\ c_i \neq 0\}|.$$

(10.2.8)定理. 如果 $(r+1)x \equiv 0 \not\equiv x \pmod{m}$，则 $w_m(x)=n$，除非 $n \equiv 0 \pmod{2}$ 并且 $x \equiv \pm[m/(r+1)] \pmod{m}$，在这种情况下 $w_m(x)=\frac{n}{2}$.

如果我们有 x 的一个 NAF，其中 $c_{n-1}=0$，则它是一个 CNAF 的附加条件就已满足。因此定理 10.2.5 蕴含着下述定理。

(10.2.9)定理. 整数 x 有一个满足 $c_{n-1}=0$ 的CNAF当且仅当存在 $y \in \mathbf{Z}$，使 $x \equiv y \pmod{m}$，$|y| \leqslant m/(r+1)$.

由这个定理导出另一个求整数模重量的方法。

(10.2.10)定理. 对 $x \in \mathbf{Z}$，我们有

$$\begin{aligned} w_m(x) = |\{j \mid 0 \leqslant j < n, \exists y \in \mathbf{Z}, \\ m/(r+1) < y \leqslant mr/(r+1), \\ y \equiv r^j x \pmod{m}\}|. \end{aligned}$$

证明. 显然，rx 的 CNAF 是 x 的 CNAF 的一个循环移位，即 $w_m(rx)=w_m(x)$。假设 $x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{m}$是一个 CNAF 且 $c_{n-1-i}=0$，则 $r^i x$ 有一个 CNAF，r^{n-1} 的系数是0。由定理 10.2.9，这种情形出现当且仅当存在 y，使 $y \equiv r^i x \pmod{m}$，$|y| <$

$m/(r+1)$. 因为模重量是非零系数的个数,所以除了定理 10.2.7 的例外情形,结论便已得到. 对于那种例外情形,利用定理 10.2.8 就可得到结论. □

§ 10.3 Mandelbaum-Barrows 码

现在我们介绍一类能纠正多个差错的循环 AN 码. 它是由 J. T. Barrows 和 D. Mandelbaum 引进的那一类码的推广. 我们首先需要一个关于循环 AN 码的模重量的定理.

(10.3.1)定理. 设 $C\subset \mathbf{Z}/(r^n-1)$ 是一个循环 AN 码, A 是其生成元. 又设

$$B:=(r^n-1)/A=|C|,$$

则

$$\sum_{x\in C}w_m(x)=n\left(\left\lfloor\frac{rB}{r+1}\right\rfloor-\left\lfloor\frac{B}{r+1}\right\rfloor\right).$$

证明. 我们假定每个 $x\in C$ 都有唯一的 CNAF

$$x\equiv\sum_{i=0}^{n-1}c_{i,x}r^i \pmod{r^n-1}.$$

如果 C 中有元素具有两种 CNAF, 只是稍微复杂一点而已. 我们把它留给读者. 我们必须确定非零系数 $c_{i,x}$ 的个数,其中 $0\leqslant i\leqslant n-1, x\in C$. 我们视 $c_{i,x}$ 为一个矩阵的元素. 由于 C 是循环码, 所以这个矩阵的每一列都有相同数目的 0. 因此, 所求之数等于 $n|\{x\in C\mid c_{n-1,x}\neq 0\}|$. 由定理 10.2.9, 我们有 $c_{n-1,x}\neq 0$ 当且仅当存在 $y\in\mathbf{Z}$, 使 $y\equiv x\pmod{r^n-1}$, $m/(r+1)<y\leqslant mr/(r+1)$. 因为 x 具有形式 $AN\pmod{r^n-1}(0\leqslant N<B)$,必有 $B/(r+1)<N\leqslant Br/(r+1)$. □

定理 10.3.1 中的表达式近似地等于 $n|C|[(r-1)/(r+1)]$, 因此该定理类似于线性码 C 的一个较早的结果 (参见(3.7.5)):

$$\sum_{\mathbf{x}\in C} w(\mathbf{x}) = n|C|\frac{q-1}{q}.$$

下面的定理引进了广义 Mandelbaum-Barrows 码，并证明这些码都是等距离码。

(10.3.2)定理． 设 B 是一个不能整除 r 的素数，使 $(\mathbf{Z}/B\mathbf{Z})$ 由元素 r 和 -1 生成．再设 n 是正整数，使得 $r^n \equiv 1 \pmod{B}$，令 $A := (r^n - 1)/B$，则由 A 生成的码 $C \subset \mathbf{Z}/(r^n - 1)$ 是一个等距离码，其距离为：

$$\frac{n}{(B-1)}\left(\left\lfloor\frac{rB}{r+1}\right\rfloor - \left\lfloor\frac{B}{r+1}\right\rfloor\right).$$

证明．设 $x\in C, x\neq 0$，则 $x \equiv AN \pmod{r^n - 1}$，而 $N \not\equiv 0 \pmod{B}$．由假设可得：存在 i，使 $N \equiv \pm r^i \pmod{B}$． 因此，$w_m(x) = w_m(\pm r^i A) = w_m(A)$． 这证明了 C 是等距离码．至于码字的重量由定理 10.3.1 即可得到． □

Mandelbaum-Barrows 码对应于 § 6.2 中的极小循环码 M_i^-．注意这些码的字长至少为 $\frac{1}{2}(B-1)$，相对于码字个数 B 而言是比较大的．因此，从实用的角度看，它们似乎并不重要．

§ 10.4 评　注

有兴趣进一步了解算术码的读者，可以参阅 W. W. Peterson 和 E. J. Weldon 的[53]，J. L. Massey 和 O. N. Garcia 的[48]，T. R. N. Rao 的[58]．完全的纠单错循环 AN 码已得到广泛研究，建议参阅 M. Goto 的[28] M. Goto 和 T. Fukumara 的[29]，以及 V. M. Gritsenko 的[31]．当 $r = 10$ 或 $r = 2^k (k > 1)$ 时，完全的纠单错循环 AN 码不存在．

关于 NAF 和 CNAF 的更详细的讨论可参阅 W. E. Clark 和 J. J. Liang 的[14]，[15]． 关于二元 Mandelbaum-Barrows 码的参考文献可以在[48]中找到． 存在一类与 BCH 码有某些相

似点的循环 AN 码. 这可以在 C. L. Chen, R. T. Chien 和 C. K. Liu 的[12]中找到.

关于算术码的更多的材料, 建议去参阅 H. W. Lenstra 在 Séminaire Delange-Pisot-Poitou (Théorie des Nombres, 1977/78) 讨论会上的一篇题为《完全算术码》的论文.

§ 10.5 问　　题

10.5.1. 证明, 如果 w 的定义如 (10.1.1), 则对每个 $A \in \mathbf{Z}$, $\min\{w(AN) \mid N \in \mathbf{Z}, N \neq 0\} \leqslant 2$.

10.5.2. 推广(10.1.4), 并找一个 $r = 3$ 的例子.

10.5.3. 考虑模 3^6-1 的三元表示. 利用定理 10.2.3 的证明方法, 找出 455 的一个 CNAF.

10.5.4. 当 $B = 11, r = 3, n = 5$ 时, 确定 Mandelbaum-Barrows 码的码字.

第十一章 卷 积 码

§ 11.1 引　　言

本章所要讨论的码与前述各章有很大的不同，它们不再是组码，即码字的长度不再是常量．尽管这种码与组码有相似和相关之处，但二者之间有着巨大的差别，即卷积码的数学理论还没有很好地发展．这也是数学家难以对它产生兴趣的原因之一．

尽管如此，在引言中，我们把卫星通讯作为应用编码理论的最引人注目的例子之一，今天这一领域的一个主要工具就是卷积码！因此，对这个课题作个简短介绍是适当的，至于组码与卷积码的比较，可以参阅[51，§ 11.4]．在结束几节介绍之后，我们将讨论这个课题的较为数学化的几个方面．卷积码的主要研究领域是减少译码复杂性．我们不打算涉及这些方面，请有兴趣的读者查阅有关文献．

在这一章里，我们假设字母是 2 元的，推广到 $\mathbf{F}_q$ 是直接的．对卷积编码的所有介绍，几乎都使用同一个例子．再加一个例子反而会使某些学生觉得没有其它例子了．因此我们将仅使用这个典范的例子．

图 4 所示的是这种码的编码装置． 三个方块是存贮单元（触发器），它们可以处于两种不同的状态之一，这两种状态分别表示为 0 和 1．整个系统由一个在每 t_0 秒都产生一个信号的外部时钟脉冲控制（为方便计，我们适当选择时间单位以使 $t_0 = 1$）．这个信号的作用在于使触发器的内部状态沿箭头方向依次移到下一个单元，因此，也称这些存贮单元为移位寄存器．图中的⊕表示模 2 加法器．对于每个时钟脉冲，第一和第三个触发器的内存相加，然后以流 T_0 离开编码器．需要处理的信息从左端以流 I_0 进入编码

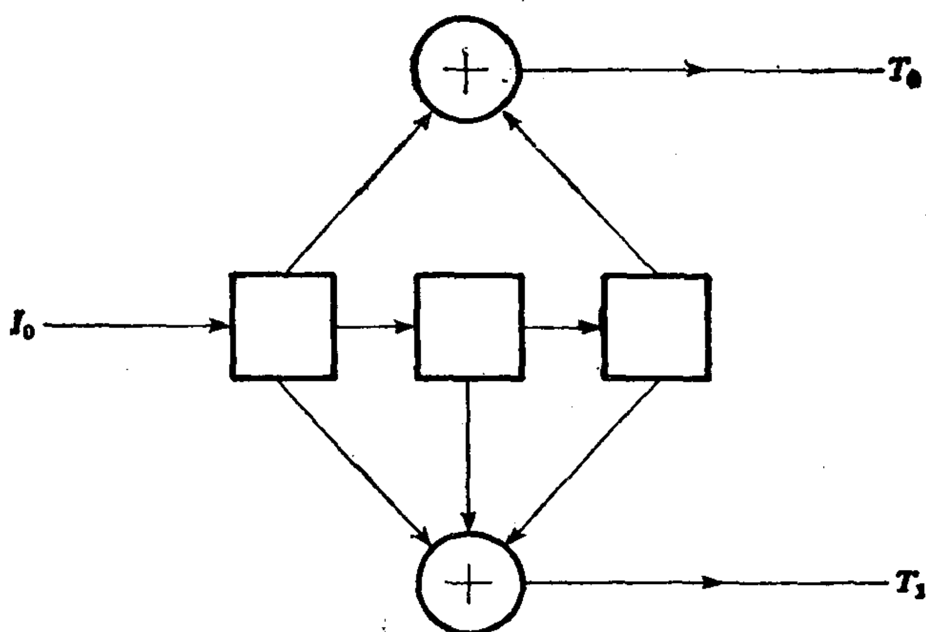


图 4

器．注意，第一个触发器实际上是多余的，因为它的作用仅是把输入流分为三个方向．移位寄存器的第二、第三个单元显示了与组码的本质区别，它们是记忆单元，保证 $t-1$ 和 $t-2$ 时的输入信号在 t 时刻仍然有效，输出依赖于这三个输入信号．在实际中，往往将输出流 T_0 和 T_1 交织产生一个新的输出流．因此，如果我们以(0,0,0)为初态，寄存器的输入流为一个 1，后面的为全 0，则寄存器先变成(1,0,0)，产生的输出是(1,1)；然后是(0,1,0)，输出(0,1)；接着是(0,0,1)，输出(1,1)；之后回到原始状态并输出一个全 0 流．

描述这个编码器动作的一个有效方法是图 5 所给出的状态图．这里第二和第三个触发器的内容称为寄存器的状态．我们用实线连接两个状态，如果寄存器输入 0 可以由一个状态变为另一个状态．同理，虚线对应于输入 1 时的关系．沿着这些边，我们在括号中标出了 T_0，T_1 处的两个输出． 一个输入流 I_0 对应着图 5 中那个图的一条道路．

这个编码过程的数学描述可如下进行．我们用系数取自 $\mathbf{F}_2$ 的形式幂级数 $I_0(x):=i_0+i_1x+i_2x^2+\cdots$ 表示输入流 $i_0,i_1,i_2,\cdots$．同理，分别用幂级数 $T_0(x)$ 和 $T_1(x)$ 表示在 T_0 和 T_1 处的输出．为

了使时间一致，我们让第一个输入对应于第一个输出. 于是显然有

$$T_0(x) = (1 + x^2)I_0(x),$$
$$T_1(x) = (1 + x + x^2)I_0(x).$$

因而 T_0 和 T_1 的交织可以描述为

$$T(x) = T_0(x^2) + xT_1(x^2).$$

在我们的例子中，输入是 $I_0(x) = 1$,输出序列是

11 01 11 00 00…

即为

$$G(x) := 1 + x + x^3 + x^4 + x^5 = (1 + (x^2)^2) + x(1 + (x^2) + (x^2)^2).$$

因此，若定义 $I(x) := I_0(x^2)$，则

$$(11.1.1)\quad T(x) = G(x)I(x).$$

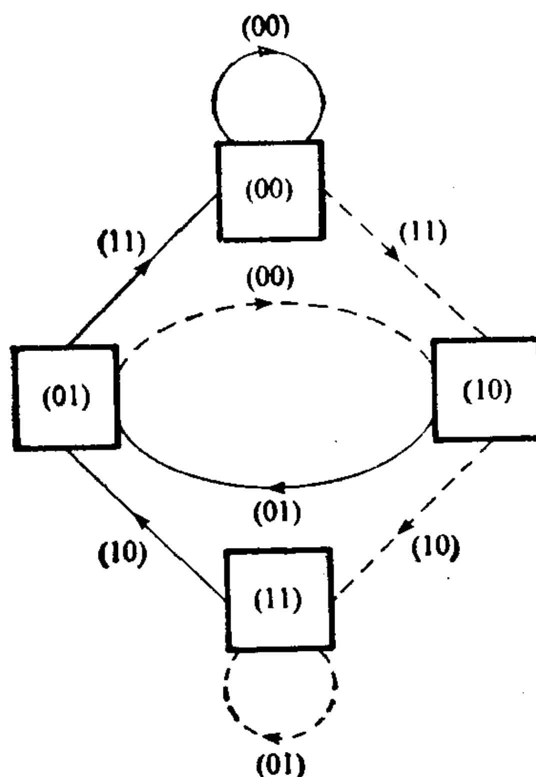


图 5

由于明显的原因，我们说这个卷积码的信息率是 $\frac{1}{2}$. 与通常一样，这个码是所有可能的输出序列 $T(x)$ 的集合. 多项式 $G(x)$ 有时也称为这个码的**生成多项式**.

由上面的描述，进入移位寄存器的信息符号 i_ν 影响了被传输序列的 6 个符号，这个数值称为码的**约束长度**. 约束长度等于 $1 + \deg G(x)$. 应该提醒读者的是，其他作者至少使用过另外两种约束长度的定义(其中之一是移位寄存器的长度，即在图 4 中它等于 3). 在我们的例子中，我们说这个例子的**记忆**为 2，因为当输入 i_ν 时，编码器必须利用前两个输入才能产生输出.

我们知道，在组码中最重要的概念之一是码的极小距离. 对于卷积码而言也有类似的概念，它也在译码研究中起至关重要的作用. 这就是码的**自由距离**，它定义为所有非零输出序列的最小

重量．在上面讨论的例子中，它等于 5，就是 $G(x)$ 的重量．

现在我们用完全类似的方法引进信息率为 $\frac{1}{n}$ 的卷积码．设有一个以级数 $I_0(x)$ 给出的信息符号序列，又有 n 个由移位寄存器输出的序列：$T_0(x), T_1(x), \cdots T_{n-1}(x)$，其中每一个序列 $T_i(x)$ 都是由 $I_0(x)$ 乘以某个多项式 $G_i(x)$ 得到的．传输序列 $T(x) = \sum_{i=0}^{n-1} x^i T_i(x)$．如前，我们定义

$$I(x) := I_0(x^n), G(x) := \sum_{i=0}^{n-1} x^i G_i(x^n),$$

则 $T(x) = G(x)I(x)$．

显然，无论从哪个角度看，多项式 $G_i(x)(i = 0, 1, \cdots, n-1)$ 的选择决定了码之性质的好坏．现在我们叙述一种明显坏的情形．假定输入流 $I_0(x)$ 包含无限多个 1，与之相应的输出流 $T(x)$ 仅有有限多个 1．如果碰巧信道在这些 1 处发生差错，则所得到的全 0 输出流，就会使接收者误认为是来自输入 $I_0(x) = 0$ 的．因此，有限多个信道差错导致了无限多个译码错误！这样的码称为**灾变码**．有一个简便的方法保证信息率 $\frac{1}{n}$ 的卷积码不是灾变码，这只要使

$$\text{g. c. d}(G_0(x), G_1(x), \cdots, G_{n-1}(x)) = 1$$

即可．众所周知，这意味着存在多项式 $a_i(x)$ $(i = 0, 1, \cdots, n-1)$ 使得 $\sum_{i=0}^{n-1} a_i(x)G_i(x) = 1$．由此可得

$$\sum_{i=0}^{n-1} a_i(x^n)T_i(x^n) = \sum_{i=0}^{n-1} a_i(x^n)G_i(x^n)I_0(x^n) = I(x),$$

即输入可由输出来确定．更进一步，$T(x)$ 中的有限个差错不会导致译码时发生无限多个错误．

有两种方法描述如何推广到率 $\frac{k}{n}$ 码．设有 k 个移位寄存器，

其输入流分别为 $I_0(x),\cdots,I_{k-1}(x)$，又设有 n 个输出流 $T_i(x)$ $(i=0,1,\cdots,n-1)$，这里 $T_i(x)$ 是用所有的移位寄存器产生的．我们先采用上面曾经使用过的方法．因此，现在要有 kn 个多项式 $G_{ij}(x)(i=0,\cdots,k-1;j=0,\cdots,n-1)$ 用于描述．我们有

$$T_j(x)=\sum_{i=0}^{k-1}G_{ij}(x)I_i(x).$$

这时仅用一个多项式已不能描述编码过程了．我们更欣赏下述描述率 $\frac{k}{n}$ 卷积码的方法，它把这种卷积码变成了一个适当选择的域上的组码．

设 $\mathscr{F}$ 是 $\mathbf{F}_2[x]$ 的商域，即所有形为

$$\sum_{i=r}^{\infty}a_ix^i\ \ (r\in\mathbf{Z},a_i\in\mathbf{F}_2)$$

的 Laurent 级数组成的域．我们把在时刻 t 进入各个移位寄存器的 k 个比特视为 $\mathbf{F}_2^k$ 中的向量．这意味着输入序列被看作 $\mathscr{F}^k$ 中的向量(象第三章一样，向量是指行向量)．现在，我们视 kn 个多项式 $G_{ij}(x)$ 为一个生成矩阵 G 的元素，当然 n 个输出序列亦可以看作是 $\mathscr{F}^n$ 中的一个元素．这引出下述的定义．

(11.1.2)定义． 率 k/n 的二元卷积码 C 是 $\mathscr{F}^n$ 的一个 k 维子空间，它有取自 $\mathbf{F}_2[x]^n$ 的一组基．这组基向量就是 G 的行．

尽管这表明了卷积码与组码的相似之处，但是利用 $\mathscr{F}$ 却给我们留下了隐患，并且对 G 的元素的限制也是相当苛刻的．实际上，所有的信息都是有限的，并且可以假设当 $t<0$ 时没有信号．这告诉我们可以不在 $\mathscr{F}$ 中工作，一切都可以在 $\mathbf{F}[x]$ 中进行．但是，$\mathbf{F}[x]$ 不是域又会带来别的困难．

在讨论组码时，我们曾经指出：对一个给定的码，G 有多种不同的选择，其中有些 G 可以使对 C 的分析较为容易．对于卷积码，这种情况也会出现．关于生成矩阵这方面的研究，我们建议读者参阅[23]．这是卷积码的很少几个数学分析的例子之一．

§ 11.2 卷积码的译码

在实际应用中，有几种卷积码的译码算法．它们或多或少地有相似之处，并且都没用到太深的数学知识．事实上，它们类似于组码译码时所用的方法：把接收字与所有码字进行简单的比较．由于卷积码是无限长的，所以必须将其截短才能比较，即仅考虑接收到的前 l 个信息符号．经过比较，我们就可以确定(比方说)第一个信息符号．然后，对随后的符号重复这个过程．我们借助图 4 和图 5 的例子更详细地叙述所谓的 Viterbi **算法**．

假设接收到的信息流是 10 00 01 10 00 ⋯．图 6 标明了在 $t = 0, 1, 2, 3$ 时的所有可能的状态，箭头表示图 5 中的通路．图 6 中的虚线在下个图中将省略．为了说明这样做的理由，我们假

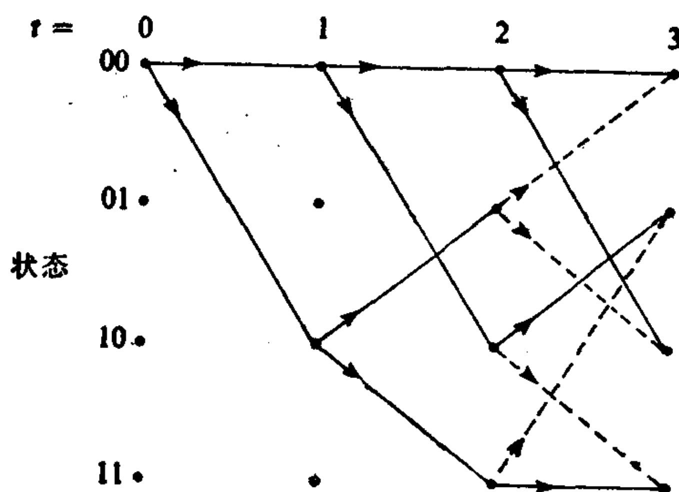


图 6

定在 $t = 3$ 时寄存器的状态是 00，进入这一状态的一条通路是对应于输出 00 00 00 ⋯ 的水平线．因此这个假设意味着在 $t = 3$ 时已出现了两个差错．另一方面，如果经由 10 和 01 进入状态 00，那么就会输出 11 01 11，便已出现了三个差错．虽然我们并不知道寄存器是否处于状态 00，但若果真如此，则水平的那条道路就更可能是走过的路线．进一步，这条道路含有两个差错．我

们把图 6 扩充成图 7，即包含 $t=4$ 和 $t=5$，还标明到达不同状态所含有的差错个数。

当然，也许可能存在两条可能性相同的到达某个状态的道路．在这种情况下，我们选择其中的一条而放弃另一条．相应于每个时刻和状态，我们总能列出相对于上述假设的最有可能的输出．利用这种方法，从图 7 可得下述的输出序列表：

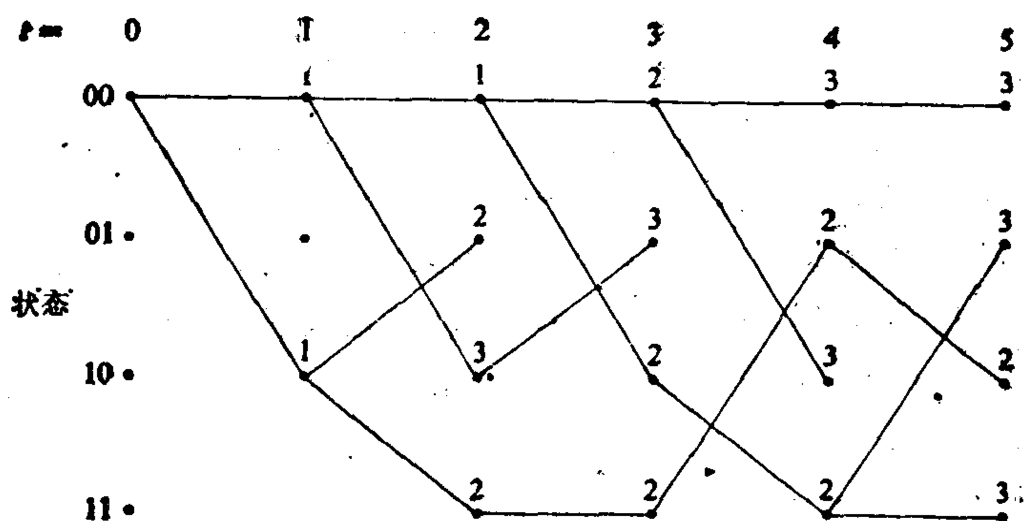


图 7

		$t=1$	$t=2$	$t=3$	$t=4$	$t=5$
状态	00	00	00 00	00 00 00	00 00 00 00	00 00 00 00 00
	01	—	11 01	00 11 01	11 10 01 10	00 00 11 10 10
	10	11	00 11	00 00 11	00 00 00 11	11 10 01 10 00
	11	—	11 10	11 10 01	00 00 11 10	00 00 11 10 01

显然，当 $t=5$ 时，按照极大似然判别法，寄存器的状态为 10．这时共出现两个差错，输出是 11 10 01 10 00．相应的输入可从图 7 找到．最简便的方法是在每条边上标出与其对应的输入符号．我们留给读者去寻找在截段部分之后继续做下去的方法．显然，我们遇到了计算时间与内存的问题．在数学上更有意义的问题是计算子序列判决译码时一次误判所产生的影响，以及确定

码的自由距离对译码精度的影响。关于这些问题的详细讨论，请读者参阅[51]。

§11.3 一些卷积码的 Gilbert 界

我们考虑一类特殊的率 k/n 卷积码，即定义如下的码。取 k 个输入序列 $I_0(x),\cdots,I_{k-1}(x)$，构造

$$I(x):=\sum_{i=0}^{k-1}x^iI_i(x^n).$$

这就是说信息比特的每一个 n 元组都以 $n-k$ 个零结尾。取一个生成多项式 $G(x)$ 并由 $T(x)=G(x)I(x)$ 定义输出。这相当于特殊地选择前述率 k/n 码中的多项式 $G_{ij}(x)$。如前，我们定义约束长度为 $l+1=1+\deg G(x)$，并且只考虑 $l+1\leqslant mn$ 的码，其中 m 是取定的。我们的兴趣在于这类码的自由距离 d_f。显然，$d_f\leqslant l+1$。通过移动时间尺度，我们在研究编码过程时可以限制 $i_0=t_0=G(0)=1$。对于输出序列的每一个初始 mn 元组 $1=t_0,t_1,\cdots,t_{mn-1}$ 和每一个初始 nk 元组 $1=i_0,i_1,\cdots,i_{mk-1}$，恰好存在一个次数 $\leqslant mn$ 的多项式 $G(x)$，使得这些初始序列与 $T(x)=G(x)I(x)$ 一致。我们想要排除那些使 $T(x)$ 的重量 $<d$ 的所有初始序列。这意味着我们至多排除 $2^{mk-1}\sum_{i=0}^{d-2}\binom{mn-1}{i}$ 个满足 $G(0)=1$ 的多项式于生成元之外。因此，当

$$2^{mk}\sum_{i=0}^{d}\binom{mn}{i}<2^{mn}$$

时，可以找到多项式 $G(x)$，它至少满足所要求的自由距离。取 $d=\lambda mn$，记 $R:=k/n$，由定理 1.4.5(i)，取对数得

$$\frac{1}{mn}\log\sum_{i=0}^{d}\binom{mn}{i}<H(\lambda)<1-R,$$

只要

$$\lambda<H^{-}(1-R).$$

这里 λ 是自由距离与约束长度之商. 这个界可与定理 5.1.9 相比较。

§ 11.4 由循环组码构造卷积码

因为人们对组码了解得更多一些，所以，很自然地有许多作者利用好的组码去构造具有所需性质的卷积码. 在这一节中，我们介绍一种已发展了的方法.

我们采用 § 4.5 的记号.

(11.4.1)引理. 设 $q=2^r, p(x)\in \mathbf{F}_q[x], c\in \mathbf{F}_q\backslash\{0\}, n\geqslant 0, N\geqslant 0$，则

$$w(p(x)(x^n-c)^N)\geqslant w((x-c)^N)\cdot w(p(x)\bmod(x^n-c)).$$

证明. 记 $p(x)$ 为 $\sum_{i=0}^{n-1} x^i Q_i(x^n)$，则由定理 4.5.2，有

$$\begin{aligned} w(p(x)(x^n-c)^N) &= \sum_{i=0}^{n-1} w(Q_i(x)(x-c)^N) \\ &\geqslant \sum_{i=0}^{n-1} w(Q_i(x))\cdot w((x-c)^N) \\ &= w((x-c)^N)\cdot w\left(\sum_{i=0}^{n-1} Q_i(c)x^i\right) \\ &= w((x-c)^N)\cdot w(p(x)\bmod(x^n-c)). \ \square \end{aligned}$$

注记. 对于任意域 $\mathbf{F}_q$，不难证明定理 11.4.1.

(11.4.2)定理. 设 $g(x)$ 是 $\mathbf{F}_q$ 上长为 n，极小距离为 d_g 的循环码的一个生成多项式，其中 $q=2^r$，n 是奇数. 又设 $h(x)$ 为这个码的奇偶校验多项式，d_h 是 $h(x)$ 所生成码的极小距离，则在同一个域上以 $G(x)=g(x)$ 为生成多项式的率 $1/2\,m$ 卷积码是非灾变的，并且满足 $d_f\geqslant\min\{d_g, 2d_h\}$.

证明.

(i) 记 $G(x)=\sum_{j=0}^{2m-1} x^j(\hat{G}_j(x^m))^2$，如果象 § 11.1 那样，考虑相

对于多项式 $G_0(x),\cdots,G_{2m-1}(x)$ 的卷积码的表示，那么对这些多项式的任何一个不可约公因子 $A(x)$，$A^2(x)$ 都能整除 $G(x)$. 但由于 n 是奇数，并且 $g(x)|x^n-1$，所以那是不可能的. 故码是非灾变的.

(ii) 考察信息序列 $I_0(x)$，有 $T(x)=G(x)I_0(x^{2m})=G(x)(\hat{I}_0(x^m))^2$，因此

$$T(x)=p(x)(g(x))^{2(i-j)+1}(h(x))^{2j},$$

其中 $i\geqslant 0$，$j\geqslant 0$，$p(x)\neq 0$，且 $p(x)$ 不被 $g(x)$ 或 $h(x)$ 整除. 再考虑两种情形:

(a) 设 $i\geqslant j$，则有

$$T(x)=p(x)(g(x))^{2(i-j)+1}(x^n-1)^{2j},$$

由引理 11.4.1，有

$$\begin{aligned}w(T(x))\geqslant\ & w((x^n-1)^{2j})\\ &\cdot w(p(x)(g(x))^{2(i-j)+1}\bmod(x^n-1))\geqslant d_g,\end{aligned}$$

这是因为第二项对应于 $g(x)$ 生成的循环码的一个码字.

(b) 设 $i<j$，则有

$$T(x)=p(x)(h(x))^{2(j-i)-1}(x^n-1)^{2i+1},$$

由

$$w((x^n-1)^{2i+1})\geqslant 2,$$

引理 11.4.1 保证了 $w(T(x))>2d_h$. □

在考察这方面的更多的例子之前，先讨论关于自由距离的一个界. 考虑 $\mathbf{F}_q$ 上的以 $G(x)=\sum_{i=0}^{n-1}x^iG_i(x^n)$ 为生成多项式的率 $1/n$ 卷积码. 设

$$L:=n(1+\max\{\deg G_i(x)\,|\,0\leqslant i\leqslant n-1\}).$$

(某些作者称这个 L 为约束长度). 显然，

$$d_f\leqslant L.$$

这个平凡的界确实相似于组码的 Singleton 界: $d\leqslant n-k+1$. 现在我们介绍一个属于 J. Justesen 的达到这个界的卷积码构造法([38]). 首先，我们证明这种情形的一个 L 的界.

(11.4.3)引理. 如果 $\mathbf{F}_q$ 上的一个卷积码率为 $1/n$ 且满足 $d_f = L$，则 $L \leqslant nq$.

证明. 如果 $d_f = L$，则每个 $G_i(x)$ 的重量都是 L/n. 我们考虑输入序列 $I_0(x) = 1 + \alpha x$，这里 α 跑遍 $\mathbf{F}_q \backslash \{0\}$，并确定相应的编码序列的平均重量 $\bar{w}$. 我们得到

$$\bar{w} = (q-1)^{-1} \sum_{\alpha \in \mathbf{F}_q \backslash \{0\}} \sum_{i=0}^{n-1} w(G_i(x)(1+\alpha x))$$

$$= (q-1)^{-1} n \left\{2(q-1) + \left(\frac{L}{n} - 1\right)(q-2)\right\}.$$

由 $\bar{w} \geqslant L$，必有 $L \leqslant nq$. □

利用类似于定理 11.4.2 的方法，我们给出一个满足 $d_f = L$ 的卷积码的简单例子.

(11.4.4)例. 设 α 是 $\mathbf{F}_4$ 的一个本原元. 又设 $g_1(x) := x^2 + \alpha x + 1, g_2(x) := x^2 + \alpha^2 x + 1$，则 $(x^5 - 1) = (x-1)g_1(x)g_2(x)$，并且 $g_1(x), g_2(x)$ 互素. 考虑由多项式

$$G(x) := g_1(x^2) + x g_2(x^2)$$

生成的 $\mathbf{F}_4$ 上的率 1/2 卷积码 C.

这个码是非灾变的. 我们把信息序列表为

$$I_0(x) = I_0'(x)(x^5 - 1)^N,$$

这里 N 达到最大. 由引理 11.4.1，我们有

$$\begin{aligned} w(T(x)) &= w(g_1(x)I_0(x)) + w(g_2(x)I_0(x)) \\ &\geqslant w((x-1)^N) \cdot \{w(g_1(x)I_0'(x) \bmod (x^5-1)) \\ &\quad + w(g_2(x)I_0'(x) \bmod (x^5-1))\}. \end{aligned}$$

现在，如果 $I_0'(x)$ 既不是 $(x-1)g_1(x)$ 的倍式，也不是 $(x-1)g_2(x)$ 的倍式，那么 BCH 界表明右端第二个因子中的两项都$\geqslant 3$. 另一方面，如果 $I_0'(x)$ 是 $(x-1)g_1(x)$ 的倍式，那么右端第二个因子中的两项都是正偶数(因为有因子 $(x-1)$). 如果其中的第二项是 2，那么再利用 BCH 界便知第一项至少为 4，因此 C 的自由距离至少为 6. 同时又有 $L = 6$. 故有 $d_f = L$.

欲推广定理 11.4.2 后面的思想,以便构造 $\mathbf{F}_q$ 上的率 $\frac{1}{2}$ 码.我们考虑形如

$$g_i(x):=(x-\alpha^m)(x-\alpha^{m+1})\cdots(x-\alpha^{m+d-2})$$

的多项式,其中 α 是 $\mathbf{F}_q$ 的一个本原元. 我们选取 $g_1(x),g_2(x)$ 为 $\left\lfloor\frac{1}{3}q\right\rfloor$ 次的且无公共零点,则 $G(x):=g_1(x^2)+xg_2(x^2)$ 生成 $\mathbf{F}_q$ 上的一个非灾变卷积码 C. 以 $g_1(x)$ 和 $g_2(x)$ 为生成元的两个循环码都具有 $\geqslant 1+\left\lfloor\frac{1}{3}q\right\rfloor=:d$ 的极小距离. 假设这两个码的校验多项式为 $h_1(x)$ 和 $h_2(x)$,则 C 的信息序列可以表为

$$I_0(x)=(x^{q-1}-1)^r(h_1(x))^s(h_2(x))^t p(x),$$

其中 $p(x)$ 不是 $h_1(x)$, $h_2(x)$ 的倍式,且 s 或 t 为零. 首先假设 $s=t=0$. 由引理 11.4.1,我们有

$$\begin{aligned}
w(T(x)) &= w(g_1(x)I_0(x))+w(g_2(x)I_0(x))\\
&\geqslant \sum_{i=1}^{2} w((x-1)^r)w(p(x)g_i(x)\bmod(x^{q-1}-1))\\
&\geqslant 2d.
\end{aligned}$$

如果 $s>0$,则类似地可得

$$\begin{aligned}
w(T(x)) &= w((x^{q-1}-1)^r(h_1(x))^s g_1(x)p(x))\\
&\quad + w((x^{q-1}-1)^r(h_1(x))^s g_2(x)p(x))\\
&\geqslant w((x-1)^{r+1})w(p(x)(h_1(x))^{s-1}\bmod(x^{q-1}\\
&\quad -1))+w((x-1)^r)w(p(x)(h_1(x))^s g_2(x)\\
&\quad \cdot \bmod(x^{q-1}-1))\\
&\geqslant 2+\left(q-\left\lfloor\frac{1}{3}q\right\rfloor\right)\geqslant 2+2\left\lfloor\frac{1}{3}q\right\rfloor=2d.
\end{aligned}$$

由码的构造,我们知道 $L=2\left(1+\left\lfloor\frac{1}{3}q\right\rfloor\right)$,因此, $d_f=L$. 这些例子表明,这是一个构造卷积码的好方法,它可以推广到率 $1/n$ 的情形. 具体细节可参阅[38].

§ 11.5 卷积码的自同构

我们已经看到(比如在介绍循环码的一章中)要求一个码在某个置换群下不变能产生有意义的进展：不仅引进了许多代数方法，而且发现了若干好码。因此，试图用类似的方法研究卷积码也十分自然。我们将粗略地讨论一些这方面的思想，并定义循环卷积码。尽管我们不打算涉及许多细节，仍希望这些讨论足以使读者决定他对这个领域是否有兴趣。建议有兴趣的读者去查阅 Ph. Piret 的工作 ([59], [55])。C. Roos 重新研究过这一工作[59]。这些思想引出了一些好码，这些都是值得进一步研究的。

我们考虑由(11.1.1)定义的一个卷积码。如果称这样一个码——同时对 x^i 的系数 a_i 作循环移位仍保持不变，这里 $a_i\in \mathbf{F}_2^n$——是循环的，那么我们不会得到任何有意义的东西。事实上，这种码就是简单的组码。这表明，找一个合理的方法定义自同构并不容易。我们的做法如下：设 K 是作用在 $\mathbf{F}_2^n$ 上的一个置换群。考虑 $K^{\mathbf{Z}}$，即所有映射 $\varphi: \mathbf{Z}\to K$ 组成的集合，通过定义

$$\varphi_1\varphi_2(n)=\varphi_1(n)\varphi_2(n)$$

可以使它成为一个群。用 φ_n 表示 $\varphi(n)$，注意 $\varphi_n\in K$。于是我们定义 φ 在 $\mathscr{F}^n$ 上的作用为

$$(11.5.1)\qquad \varphi\left(\sum_{i=r}^{\infty} \mathbf{a}_i x^i\right):=\sum_{i=r}^{\infty}\varphi(\mathbf{a}_i)x^i.$$

(11.5.2)定义. 设 C 是一个卷积码，则 $K^{\mathbf{Z}}$ 中所有满足条件 $\varphi(C)=C$ 的 φ 组成的集合叫做 C 的**自同构群**.

由卷积码的定义，显然，用 x 乘码 C 保持其不变。因此，如果 φ 是 C 的一个自同构，则 $\varphi^x:=x^{-1}\varphi x$ 也是 C 的自同构。进一步，如果我们仅考虑在一个固定位置上的作用，比如说 φ_i，那么显然就可以得到 $\mathbf{F}_2^n$ 上的一个置换群，它是 C 的自同构群在第 i 个坐标上的投影。由我们前面的注记以及 $\varphi_i^x(\mathbf{a}_i)=\varphi_{i+1}(\mathbf{a}_i)$ 这一事实，我们看到所有的投影都是相同的群。所以很自然地希望找到

投影是循环群的码．为此，我们要利用研究组码的代数方法．引进变量子，并且视 $\mathbf{F}_2^n$ 为 $\mathbf{F}_2[z]\bmod(z^n-1)$．设 π 是一个整数，满足 $(\pi,n)=1$．又设 σ 是 $\mathbf{F}_2^n$ 的一个自同构，定义为 $\sigma: f(z)\to f(z^\pi)$．$\mathscr{F}^n$ 的元素可以表为 $\sum_{i=r}^{\infty} a_i x^i$，其中 $a_i=a_i(z)$ 是次数 $<n$ 的多项式 $(i\in\mathbf{Z})$．在 $\mathscr{F}^n$ 中用显然的方法定义加法，乘法（记为 $*$）定义为

$$(11.5.3)\qquad \sum_i a_i x^i * \sum_j b_j x^j := \sum_i \sum_j \sigma^j(a_i) b_j x^{i+j}.$$

假定我们取左边的因子为 z（即 $a_0=z$，$a_i=0$，$i\neq 0$），则由 (11.5.3) 有

$$(11.5.4)\qquad z * \sum_j b_j x^j = \sum_j (z^{\pi^j} b_j) x^j.$$

即 x^j 的系数 b_j 循环移动了 $\pi^j(\bmod n)$ 个位置．上述定义的要点是：$(\mathscr{F}^n,+,*)$ 是一个代数．记之为 $\mathscr{A}(n,\pi)$．

(11.5.5)定义． 一个循环卷积码（记为 CCC）是代数 $\mathscr{A}(n,\pi)$ 的一个左理想，它有一组由多项式组成的基．

显然，由(11.5.4)，现在我们的确找到了这样一种码，它的自同构群在任一坐标上的投影都是循环群．与平凡情形的差别在于对每个位置的循环移位不是一样的．我们举例说明有一类非平凡的对象值得研究．令

(11.5.6)

$$G=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1+x & 1 & 1 & x & 1 & x & x \\ 0 & 1 & 1+x & 1 & x & 1+x & x \\ 0 & x & 1 & 1+x & 1+x & x & 1 \end{bmatrix},$$

由 G 来定义一个率 $\frac{4}{7}$ 的单记忆 2 元卷积码．先视 $\mathbf{F}_2^7$ 为 $\mathbf{F}_2[z]$ $\bmod(z^7-1)$．记 $z^7-1=(1+z)(1+z+z^3)(1+z^2+z^3)=m_0(z)m_1(z)m_3(z)$，则 G 可以简记为

$$G = \begin{bmatrix} m_1 m_3 \\ m_0 m_3 \\ z m_0 m_3 \\ z^2 m_0 m_3 \end{bmatrix} + \begin{bmatrix} 0 \\ m_0^3 m_1 \\ z^{-1} m_0^3 m_1 \\ z^{-2} m_0^3 m_1 \end{bmatrix} x. \tag{11.5.7}$$

我们断言：G 是 $\mathscr{A}(7,-1)$ 中的一个 CCC 的生成矩阵．因为 $\pi=-1$，由(11.5.4)我们有

$$z * \sum_i c_i x^i = \sum_i (z^{(-1)^i} c_i) x^i. \tag{11.5.8}$$

为了证明这个码是 CCC，只需考察码字 $(1000)G$，$(0100)G$，$(0010)G$，$(0001)G$，在它们左边乘以 z，然后证明这些乘积仍在码内．利用形(11.5.7)，(11.5.8)，前三个都是明显的．例如

$$\begin{aligned} z*(0100)G &= z*(m_0 m_3 + m_0^3 m_1 x) \\ &= z m_0 m_3 + z^{-1} m_0^3 m_1 x = (0010)G. \end{aligned}$$

此外

$$\begin{aligned} z*(0001)G &= z*(z^2 m_0 m_3 + z^{-2} m_0^3 m_1 x) \\ &= z^3 m_0 m_3 + z^{-3} m_0^3 m_1 x \\ &= (1+z) m_0 m_3 + (1+z^6) m_0^3 m_1 x \\ &= (0110)G. \end{aligned}$$

Piret 理论的要点是要证明：一个 CCC 总有一个类似于(11.5.7)的形式简单的生成矩阵．这使我们有可能用相对容易些的办法构造一些例子，以研究它们的性质，比如它们的自由距离．

§11.6 评　　注

卷积码是 P. Elias 在 1955 年引进的([20])．关于卷积码是否比组码"更好"的争论也不少．尽管缺乏深入的数学理论，但卷积码在实际应用上却是很成功的．这些码有许多几乎是随机选取的．为了进行一次外层空间的卫星计划([1])，人们提出了将组码和卷积码相结合的设想．具体地说，是取一个信息流，将其分成长为 12 比特的组，再将这些组用扩充的([24,12]) Golay 码进行编

码，所得的信号流就作为卷积码编码器的输入．这与§9.2中的级联码的思想是一致的．

关于拟循环组码与卷积码的联系，建议读者去阅读 G. Solomon 和 H. C. A. van. Tiborg 的论文[66]．他们证明了 Golay 码可以按卷积方式进行编码和译码．

在§3.2中，我们已经看到，在组码的译码过程中，估计差错模式不依赖于所传送的字．其思想是引入校验子（见(3.2.6)）．同样的思想已成功地应用于卷积码．关于这一方法的更多的讨论，可参阅 J. P. M. Schalkwijk, A. J. Vinck 和 K. A. Post 的论文[60]．有关卷积码译码出错的概率的一些结果，可以在[51,§9.3]中找到．

§11.7 问　　题

11.7.1. 假设在图4中去掉第三个触发器与 T_1 的加法间的连线，证明所得的是实变码．

11.7.2. 设 $g(x)$ 是一个极小距离为 d 的循环码的生成多项式．象§11.1中那样，取两个多项式 $G_0(x)$ 和 $G_1(x)$，生成一个率 $\frac{1}{2}$ 卷积码．如果这两个多项式满足 $g(x)=G_0(x^2)+xG_1(x^2)$，那么由(11.1.1)，所有的编码序列都是 $g(x)$ 的倍式．举一个例子，使其自由距离小于 d．构造如图4的编码器检验所得的结果．

11.7.3. 确定由(11.5.7)给出的 CCC 的自由距离．

问题的提示与解答

第二章

2.4.1.
$$\sum_{0\leqslant k<N/2}\binom{N}{k}q^kp^{N-k}<(pq)^{N/2}\sum_{0\leqslant k<N/2}\binom{N}{k}$$
$$=2^{N-1}(pq)^{N/2}<(0.07)^N.$$

2.4.2 有 64 种可能的差错模式. 我们知道其中的 8 个在译码后产生 3 个正确的信息符号.为了分析其余的差错模式,应该明确指出只有 4 个本质上不同的 3 元组 (s_1, s_2, s_3). 考虑其可能性之一, 比如说 $(s_1, s_2, s_3)=(1, 1, 0)$. 这可由差错模式(101011), (011101),(110000),(010011),(100101),(000110), (111110) 得到, 也可由(001000)得到, 这是可能性最大的一个. 我们的判别是假设 $e_3=1$. 这样, 就得到产生两个正确信息符号的概率是 $p^2q^4+2p^4q^2$, 产生一个正确信息符号的概率是 $2p^3q^3+p^5q$. 以同样的方法分析其它情形,我们发现信息符号被译错的概率为

$$\frac{1}{3}(22p^2q^4+36p^3q^3+24p^4q^2+12p^5q+2p^6)$$

$$=\frac{1}{3}(22p^2-52p^3+48p^4-16p^5).$$

在我们的例子中,这个值等于 0.000007,而不进行编码时为 0.001.

2.4.3. 取具有下述形式的所有 7 元组作为码字:

$$(a_1, a_2, a_3, a_2+a_3, a_1+a_3, a_1+a_2, a_1+a_2+a_3).$$

在上一问题中码的 8 个码字上附加一个符号就可以得到这个码, 这个附加符号是码字前 6 个符号之和. 这使得任何两个不同的码字在偶数个位置上相异. 即 $d(x,y)\geqslant 4$,只要 x,y 互异.

对差错模式的分析,与 § 2.1 的讨论类似. 对于 $(e_1, e_2, \cdots, e_7)$,我们有:

$$e_2 + e_3 + e_4 = s_1,$$
$$e_1 + e_3 + e_5 = s_2,$$
$$e_1 + e_2 + e_6 = s_3,$$
$$e_1 + e_2 + e_3 + e_7 = s_4.$$

(s_1, s_2, s_3, s_4) 共有16种可能，其中的 8 个可以解释为由一个无错或1-错的差错模式产生．对于其余部分中的 7 个，每一个可以解释为用三个不同的含两个错的差错模式产生．例如 $(s_1, s_2, s_3, s_4) = (1,1,0,0)$ 所对应的 $(e_1, e_2, \cdots, e_7)$ 是(0010001)，(1100000)，(0001100)．(1,1,1,0)的最有可能的解释是出现了三个差错．因此，正确的译码概率为

$$q^7 + 7q^6p + 7q^5p^2 + q^4p^3.$$

大约为 $1-14p^2$，即这个码并不比前面提到的码好多少，尽管它的信息率更小．

2.4.4. 对于重复符号的码，正确接收一个重复符号的概率为 $1-p^2$．因此，长为 6、码字为 $(a_1, a_2, a_3, a_1, a_2, a_3)$ 的码，其正确接收的概率为 $(1-p^2)^3 = 0.97$．问题 2.4.2 中的码具有性质：任何两个码字在三个位置上不同．所以两次删除不致于造成损害．事实上，对所有可能的具有三个删除的删除模式的分析表明，其中有 16 种情形亦无损害．这就是说，正确接收的概率为

$$(1-p)^3 = (1 + 3p + 6p^2 + 6p^3) = 0.996.$$

考虑到两个码非常相似这样一个事实，所以这是一个显著的改进．

第三章

3.7.1. 由(3.1.6)我们有 $\sum_{i=0}^{3} \binom{n}{i} = 2^l$，对某个整数 l．这个方程约简为 $(n+1)(n^2-n+6) = 3.2^{l+1}$，即

$$(n+1)\{(n+1)^2 - 3(n+1) + 8\} = 3.2^{l+1}.$$

如果 $n+1$ 能被 16 整除，则左边的第二个因子能被 8 而不能被 16 整除，即该因子为 8 或 24．矛盾．因此，$n+1$ 是 24 的因子．由 $n \geq 7$，我们看到只能 $n = 7, 11$ 或 23．但是 $n = 11$ 不满足方

程．对 $n=7$，码 $M=\{\mathbf{0},\mathbf{1}\}$ 就是一个例子． $n=23$ 的情形见 § 4.2。

3.7.2. 设 $\mathbf{c}\in C, w(\mathbf{c})\leqslant n-k$,则 $\mathbf{c}$ 有 k 个位置的坐标为 0．因为 C 关于这 k 个位置是系统的,所以 $\mathbf{c}=\mathbf{0}$．因此，$d>n-k$．给定 k 个位置,则有一些码字在这 k 个位置中的 $k-1$ 个为零,即 $d\leqslant n-k+1$． 为了与 § 3.2 中所给的可分定义一致，称一个 $[n,k,n-k+1]$ 码为**极大距离可分码**(MDS 码)．

3.7.3. 因为 $C\subset C^{\perp}$,所以每个 $\mathbf{c}\in C$,都有 $\langle\mathbf{c},\mathbf{c}\rangle=0$ 的性质．即 $w(\mathbf{c})$ 是偶数．因此 $\langle\mathbf{c},\mathbf{1}\rangle=0$． 然而由于字长为奇数，所以 $\langle\mathbf{1},\mathbf{1}\rangle=1$,故可将 C 中所有码字都加上 $\mathbf{1}$ 而得到 $C^{\perp}\backslash C$.

3.7.4. $|B_1(\mathbf{x})|=1+6=7$．因为 $7|C|=63<2^6$,我们可以认为存在这样的码 C．但是如果这样的 C 存在，那么根据鸽笼原理，C 中码字的某些 6 元组在最后两个位置上符号相同．去掉这些相同符号得到一个 2 元码 C'，它有 3 个码字,字长为 4,极小距离为 3．不失一般性，假定其中之一是 $\mathbf{0}$,则其余两个码字的重量 $\geqslant3$,因此二者的距离 $\leqslant2$．矛盾．

3.7.5. 由初等线性代数,对每个 i 都可以找到 C 的一组基，使其中的 $k-1$ 个基向量在第 i 个位置是0,而余下的那个基向量在 i 处为 1．因此,恰有 q^{k-1} 个码字在第 i 个位置是零．

3.7.6. C 的偶重量子码可由 C 的奇偶校验阵添上行向量 $\mathbf{1}$ 确定．这使码 C 的维数减少 1．

3.7.7. 对 $\mathbf{c}\in C$,由生成矩阵可得

$$c_1+c_2+c_5=c_3+c_4+c_6=c_1+c_2+c_3+c_4+c_7=0.$$

因此,三个接收字的校验子

$$(s_1,s_2,s_3)=(e_1+e_2+e_5,\ e_3+e_4+e_6,\ e_1+e_2+e_3+e_4+e_7),$$

分别为$(0,0,0)$,$(0,0,1)$,$(1,0,1)$．因此 (a) 是一个码字;由极大似然译码方法,(b)在第 7 个位置有一个错;(c)在位置 1 有一个错或在位置 2 有一个错,我们可取定其中之一．

3.7.8. (i) 如果 $p\equiv1(\mathrm{mod}4)$,则存在 $\alpha\in\mathbb{F}_p$,使 $\alpha^2=-1$．因

此，$G=(I_4,\alpha I_4)$ 是所求码的生成矩阵。

(ii) 如果 $p\equiv 3(\mathrm{mod}4)$，由于 $\mathbf{F}_p$ 的元素不都是平方元，故有 α 为平方元(比如 $\alpha=\beta^2$)，而 $\alpha+1$ 不是平方元，即 $\alpha+1=-\gamma^2$。于是 $\beta^2+\gamma^2=-1$，则

$$G=\begin{bmatrix}1&0&0&0&\beta&\gamma&0&0\\0&1&0&0&-\gamma&\beta&0&0\\0&0&1&0&0&0&\beta&\gamma\\0&0&0&1&0&0&-\gamma&\beta\end{bmatrix}$$

即为所求。

(iii) 若 $p=2$，请看(3.3.3)。

3.7.9. $$R_k=\frac{n-k}{n}=\frac{2^k-1-k}{2^k-1}\to 1,\text{当 } k\to\infty.$$

3.7.10. (i) 设 $(\bar{A}_0,\bar{A}_1,\cdots,\bar{A}_n,\bar{A}_{n+1})$ 是 $\bar{C}$ 的重量分布，则 $\bar{A}_{2k-1}=0$ 且 $\bar{A}_{2k}=A_{2k-1}+A_{2k}$. 因为

$$\sum A_{2k}z^{2k}=\frac{1}{2}\{A(z)+A(-z)\}$$

以及

$$\sum A_{2k-1}z^{2k-1}=\frac{1}{2}\{A(z)-A(-z)\},$$

我们有

$$\bar{A}(z)=\frac{1}{2}\{(1+z)A(z)+(1-z)A(-z)\}.$$

(ii) 由 (i) 及(3.5.2)，我们可以求出长为 $n+1=2^k$ 的扩充 Hamming 码的重量计数子为

$$\frac{1}{2}\left\{\frac{(1+z)^{n+1}+(1-z)^{n+1}}{n+1}\right\}+\frac{n}{n+1}(1-z^2)^{(n+1)/2}.$$

现在应用定理 3.5.3，对偶码的重量计数子为 $1+2nz^{(n+1)/2}+z^{n+1}$. 即除了 $\mathbf{0}$ 和 $\mathbf{1}$ 之外，该码的码字重量都是 2^{k-1}.

3.7.11 差错模式是一个非零码字 $\mathbf{c}$. 如果 $w(\mathbf{c})=i$，则这个差错模式出现的概率为 $p^i(1-p)^{n-i}$. 因此，一个差错未被检

出的概率为 $(1-p)^n\{-1+A(p/(1-p))\}$.

3.7.12. 设 $G_i(i=1,2)$ 是 C_i 的标准形式的生成矩阵. 定义 $A_{ij}\in\mathscr{R}(1\leqslant i\leqslant k_1,\ 1\leqslant j\leqslant k_2)$ 如下：除第 i 行外，A_{ij} 的前 k_1 行是 $\mathbf{0}$,而第 i 行等于 G_2 的第 j 行. 类似地选取前 k_2 列，其第 j 列是 G_1 的第 i 行的转置. 易见这唯一决定了 $\mathscr{R}$ 的元素 A_{ij}[1]. A_{ij} 是 $\mathscr{R}$ 的 k_1k_2 个线性无关元素，它们生成一个码 C. 如果 $A\in C$ 有一个非零行,那么它的重量 $\geqslant d_1$,即 A 至少有 d_1 个列的重量 $\geqslant d_2$. 于是,C 的极小距离 $\geqslant d_1d_2$,事实上等号成立.

3.7.13. 在位置 1, 9 和 10 处的子码是重复码，它是完全的 1-纠错码. 在其余 7 个位置上的子码是([7,4]) Hamming 码,也是完全码. 因此，我们有唯一的方式去纠正发生在这两个位置子集之一中的至多一个差错. C 的极小距离为 3,覆盖半径为 2.

3.7.14. (i) 考虑断语 A_k: ＝“在 2^k 个选择之后，我们得到一个线性码. 并且对 $i<k$,当 2^i 步之后码字长度增加.” 当 $k=1$ 时,断语为真. 假设对某个 k,A_k 为真,而选择的码字表如下:

$$A\begin{cases}\mathbf{c}_0=00\cdots00\cdots0\\ \vdots\\ \mathbf{c}_{2^{k-1}-1}=**\cdots10\cdots0\end{cases}$$

$$B\begin{cases}\mathbf{c}_{2^{k-1}}=**\cdots*11\cdots1\\ \vdots\\ \mathbf{c}_{2^{k}-1}=**\cdots*11\cdots1\end{cases}$$

其中 B 组的字是将 $\mathbf{c}_{2^{k-1}}$ 加到 A 组的字上而得到的. 如果 $\mathbf{c}_{2^k}$ 与 B 中的字有同样的长度,由于按字典序 $\mathbf{c}_{2^k}$ 是较大者,$\mathbf{c}_{2^k}$ 就必有形式 $\mathbf{c}_{2^{k-1}}+\mathbf{x}$,其中 $\mathbf{x}$ 在后面的位置上为 0. 然而，$d\leqslant d(\mathbf{c}_{2^{k-1}}+\mathbf{x},\mathbf{c}_{2^{k-1}}+\mathbf{c}_i)=d(\mathbf{x},\mathbf{c}_i)$，其中 $0\leqslant i\leqslant 2^{k-1}$. 这表明应选择 $\mathbf{x}$ 而不是 $\mathbf{c}_{2^{k-1}}$，矛盾. 因此，在我们选择 $\mathbf{c}_{2^k}$ 时，长度增加. 现在假定已经证明 $\mathbf{c}_{2^k+i}=\mathbf{c}_{2^k}+\mathbf{c}_i,0\leqslant i<j$ (这对于 $i=0$ 为真),我们就有 $d(\mathbf{c}_{2^k}+\mathbf{c}_i,\ \mathbf{c}_{2^k}+\mathbf{c}_j)=d(\mathbf{c}_j,\ \mathbf{c}_i)\geqslant d$，$d(\mathbf{c}_{2^k}+\mathbf{c}_j,\ \mathbf{c}_i)$

1) 事实上,若记 $\mathbf{a}_i$ 为 G_1 的第 i 行,$\mathbf{b}_j$ 为 G_2 的第 j 行,则 $A_{ij}=\mathbf{a}_i^{\prime}\mathbf{b}_j$. 并且,原书该题解有误. ——译者注

$= d(\mathbf{c}_{2^k}, \mathbf{c}_j + \mathbf{c}_i) \geqslant d$，这由于线性的假设告诉我们，有某个 v，使 $\mathbf{c}_j + \mathbf{c}_i = \mathbf{c}_v$. 于是，说明 $\mathbf{c}_{2^k} + \mathbf{c}_j$ 是 $\mathbf{c}_{2^k+j}$ 的一个可能的选择. 困难之处在于证明这是一个最小选择. 相反，假设应当选择 $\mathbf{c}_{2^k} + \mathbf{x}$，其中 $\mathbf{c}_{2^k} + x \prec \mathbf{c}_{2^k} + \mathbf{c}_j$（我们用$\prec$表示字典序）. 由归纳假设，$\mathbf{x} \succ \mathbf{c}_j$. 这些不等式表明 $\mathbf{c}_j, \mathbf{x}, \mathbf{c}_{2^k}$ 具有形式

$$\mathbf{c}_j = * \cdots * 0 a_1 a_2 \cdots a_t 00 \cdots 0$$

$$\mathbf{x} = * \cdots * 1 a_1 a_2 \cdots a_t 00 \cdots 0$$

$$\mathbf{c}_{2^k} = * \cdots * 1 * * \cdots\cdots\cdots\cdots * 1.$$

$\mathbf{c}_{2^k} + \mathbf{x}$ 是容许选择的假设意味着（再一次利用线性性）

$$d(\mathbf{c}_{2^k} + \mathbf{x}, \mathbf{c}_j + \mathbf{c}_i) \geqslant d，\text{对 } 0 \leqslant i < 2^k,$$

即

$$d(\mathbf{c}_{2^k} + \mathbf{x} + \mathbf{c}_j, \mathbf{c}_i) \geqslant d，\text{对 } 0 \leqslant i < 2^k.$$

但是，$\mathbf{c}_{2^k} + \mathbf{x} + \mathbf{c}_j \prec \mathbf{c}_{2^k}$，即 $\mathbf{c}_{2^k}$ 的选择不是最小的. 矛盾. 断语 A_k 由归纳法证明完毕.

(ii) 现在考虑 $d = 3$ 的情形. 设 n_k 是 2^k 个向量选择之后的码长，则 $n_1 = 3$. 设 C_k 是第 2^k 次选择后的线性码. 如果 C_k 不是完全的，那么存在长为 n_k 的向量 $\mathbf{x}$，它到 C_k 的每个码字的距离 $\geqslant 2$. 因此 $(\mathbf{x}, 1)$ 是 $\mathbf{c}_{2^k}$ 的一个可能的选择. 这告诉我们 $n_{k+1} = n_k + 1$. 另一方面，如果 C_k 是完全的，那么显然 $n_{k+1} = n_k + 2$，且 $\mathbf{c}_{2^k} = (100 \cdots 011)$. 断语 B_a: = “长度 $n_k = 2^a + i$，对 $k = a + i + 1$ 且 $1 \leqslant i < 2^a$” 由上述讨论及归纳法即可得到. B_a 中提到的每一个序列最终的码必定是 Hamming 码.

第四章

4.7.1. 由(4.5.6)，$\mathscr{R}(1,m)$ 的维数是 $m + 1$，即含有 2^{m+1} 个长为 $n = 2^m$ 的码字. 由定理 4.5.9，AG$(m,2)$ 的 $2(2^m - 1)$ 个超平面中的任何一个都导出 $\mathscr{R}(1,m)$ 的一个码字，即除 **0**,**1** 外的每个码字都是一个超平面的特征函数. 取 **0** 和相应于通过原点的超平面的码字，在这些码字中用 -1 代替 0. 因为任意两个超平面相交于 2^{m-1} 个点，故 n 个向量是两两正交的.

4.7.2. 因为码是完全的，所以 $\mathbb{F}_3^{11}$ 中的每个重为 3 的字都与一个重为 5 的码字距离为 2。因此，

$$A_5 = 2^3\binom{11}{3}\Big/\binom{5}{2} = 132.$$

用 $B(\mathbf{x})$ 表示相对于 $\mathbf{x}$ 的 5-集，设 $\mathbf{x},\mathbf{y}$ 都是重为 5 的码字，$\mathbf{y} \notin \{\mathbf{x}, 2\mathbf{x}\}$. 如果 $|B(\mathbf{x}) \cap B(\mathbf{y})| > 3$，那么 $w(\mathbf{x}+\mathbf{y}) + w(2\mathbf{x}+\mathbf{y}) \leqslant 8$. 这是不可能的，因为 $\mathbf{x}+\mathbf{y}$ 和 $2\mathbf{x}+\mathbf{y}$ 都是码字。故 66 个集 $B(\mathbf{x})$ 覆盖了 $66 \cdot \binom{5}{4} = \binom{11}{4}$ 个 4-子集，即全部 4-子集。

4.7.3. 由定理 1.3.8，A 的任意两行之间的距离为 6，并且经过符号的置换之后它们是 (111,111,000,00) 和(111,000,111,00). A 的其它的行一定具有形式 (100, 110, 110, 10) 或 (110, 100, 100,11)。考虑 66 个码字 $\mathbf{x}_i$, $\mathbf{x}_j + \mathbf{x}_k$, 我们有 $d(\mathbf{x}_i, \mathbf{x}_i + \mathbf{x}_k) = w(\mathbf{x}_k) = 6$, $d(\mathbf{x}_i, \mathbf{x}_j + \mathbf{x}_k) = w(\mathbf{x}_i + \mathbf{x}_j + \mathbf{x}_k) = 4$ 或 8. 这里，我们用到了上述标准表示。最后，再两次应用上述的标准形式(对任何 3 元组 $\mathbf{x}_i$, $\mathbf{x}_j$, $\mathbf{x}_k$), 我们有 $d(\mathbf{x}_i + x_j, \mathbf{x}_k + \mathbf{x}_l) \geqslant 4$. 因为 $d(\mathbf{x}, \mathbf{1}+\mathbf{y}) = 11 - d(\mathbf{x},\mathbf{y})$，所以，将 66 个码字补添进这个集合后，极小距离减为 3.

4.7.4. 将 § 4.1 的构造法应用于 17 级 Palay 矩阵。

4.7.5. G 的每个行的重量为 8 或者 12，并且任意两行是正交的。因此，G 生成一个[24,12]自对偶码 C. 由问题 4.7.3 的解答，我们知道 A 的两行之和重为 6，A 的三行之和重为 4 或 8，A 的四行之和重量至少为 4. 因为 G 的行重量都是 4 的倍数，所以 C 的码字的重量也是 4 的倍数。而且上述讨论表明，码的极小距离不会是 4，即只能是 8. 由于$(24, 2^{12}, 8)$码是唯一的，我们因此而完成了证明。

4.7.6. 设 C 是 (n, M, d) 码，d 是偶数。删减 C 得到的新码 C' 是 $(n-1, M, d-1)$ 码(只要我们用适当的方法来删减). 码 $\bar{C}'$ 是 (n, M, d) 码，因为 $\bar{C}'$ 中的所有码字都具有偶重量。

4.7.7. 设 R, S 都是 3×3 矩阵，记

$$\begin{bmatrix} R & S & S & S \\ S & R & S & S \\ S & S & R & S \\ S & S & S & R \end{bmatrix} =: M(R,S).$$

A,B,C,D 的行重量分别为5,6,8,9. 对两个码字 $\mathbf{a}$, $\mathbf{b}$, 我们有 $d(\mathbf{a},\mathbf{b}) = w(\mathbf{a}) + w(\mathbf{b}) - 2\langle\mathbf{a},\mathbf{b}\rangle$,这里$\langle\mathbf{a},\mathbf{b}\rangle$在$\mathbf{Z}$中计算. 由分块乘法,有

$AA^T = M(4I + J, 2J)$, $BB^T = M(3I + 3J, 3J - I)$,

$AB^T = M(5J, 3J) - 2B^T$, 一个以 3 或 1 为元素的矩阵.

这说明, A 或 B 中任意两行之间的距离为 6 或 8, 而 A 的任意一行与 B 的任意一行之间的距离为 5 或 9. 用同样的方法, 由

$CA^T = (4J - 2I, 4J - 2I, 4J - 2I, 4J - 2I)$,

$CB^T = (4J, 4J, 4J, 4J)$,

$DA^T = 3J + D$, $DB^T = 3J + 2D$,

$CC^T = 4J + 4I$, $DD^T = 3I + 6J$, $DC^T = 6J$,

可得余下的距离至少是 5. (这个构造属于 J. H. van Lint, 见[43].)

4.7.8. 由定理 1.3.8,我们有 $A^T = -A$ 及 $AA^T = 11I$. 这说明在 $\mathbf{F}_3$ 上, G的任意两行的内积为零, 即G生成一个[24,12]自对偶码 C. 因此, (A,I) 也是码C的生成矩阵. 所以, 在寻找具有极小重量的码字时,可以假设该码字的前 12 个位置的重量至多占全部重量的一半. 因为C是自对偶的,所以每个码字的重量都是 3 的倍数. G的每个行的重量为 $1+11 = 12$, 两个行的线性组合的重量为 $2 + 7=9$ (这可由 $AA^T = 11I$ 得到). 因此,三个行的线性组合的重量至少为 $3 + (11-7)$,因而至少为 9. 这说明C的极小重量为 9.

注记. 这个码和三元 Golay 码都是对称码的例子, 它们是由 V. Pless 引进的(1972). 在这样的码中, 固定码字的重量常常可以导出一个 t-设计(甚至 $t = 5$), 就如同问题 4.7.2 那样. 有兴趣的读者可参阅[11].

4.7.9. 设 $\mathbf{1}, \mathbf{v}_0, \cdots, \mathbf{v}_{m-1}$ 是 $\mathscr{R}(1, m)$ 的基向量．由(4.5.3)之 (i),(iii)，我们知道 $\mathbf{1} = (\mathbf{1}.\mathbf{1})$, $\mathbf{w}_0 = (\mathbf{v}_0, \mathbf{v}_0), \cdots, \mathbf{w}_{m-1} = (\mathbf{v}_{m-1}, \mathbf{v}_{m-1})$, $\mathbf{w}_m = (\mathbf{0}, \mathbf{1})$ 是 $\mathscr{R}(1, m+1)$ 的基向量（长度为 2^{m+1}）．因此，$\mathscr{R}(r+1, m+1)$ 的形如 $\mathbf{w}_{i_1}, \cdots, \mathbf{w}_{i_s}$ 的一个基向量一定是 $(\mathbf{u}, \mathbf{u})$ 型的或者是 $(\mathbf{0}, \mathbf{v})$ 型的． 这里 $\mathbf{u}$ 是 $\mathscr{R}(r+1, m)$ 的基向量，$\mathbf{v}$ 是 $\mathscr{R}(r, m)$ 的基向量．当 $\mathbf{w}_m$ 不在乘积中出现时为前者，否则为后者．如果 $d(r, m)$ 是 $\mathscr{R}(r, m)$ 的极小距离,则由 $(\mathbf{u}, \mathbf{u}+\mathbf{v})$-构造,我们知道,

$$d(r+1, m+1) = \min\{2d(r+1, m), d(r, m)\}.$$

于是由归纳法证明了定理 4.5.7 成立．

4.7.10. (i) 将向量 $\mathbf{x}^*$ 和 $\mathbf{c}^* = \pm \mathbf{a}_i$ 看作 $\mathbf{R}^n$ 中的向量． 显然,$\langle \mathbf{x}^*, \mathbf{c}^* \rangle = n - 2d(\mathbf{x}, \mathbf{c})$．我们可以假定 $\mathbf{a}_i$ 的选择使$\langle \mathbf{x}^*, \mathbf{a}_i \rangle$ 是正的 $(1 \leqslant i \leqslant n)$．向量 $\mathbf{x}^*$ 和全部 $\mathbf{a}_i$ 的长度都是 $\sqrt{n}$． 因此，由 $\mathbf{a}_i$ 两两正交知 $\sum_{i=1}^{n} \langle \mathbf{x}^*, \mathbf{a}_i^* \rangle^2 = n^2$．于是存在 i,使 $\langle \mathbf{x}^*, \mathbf{a}_i \rangle \geqslant \sqrt{n}$．

(ii) 现在设 $m = 2k, \mathbf{c} \in \mathscr{R}(1, m)$．由定义，$\mathbf{c}$ 是 $\mathbf{F}_2^m$ 上的一个线性函数的真值表,因此,$d(\mathbf{x}, \mathbf{c})$ 是 $\mathbf{F}_2^m$ 中使 $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}$ 与这个线性函数的和取值为 1 的点的个数． 注意到

$$\begin{aligned} & x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + x_1 \\ = & x_1\bar{x}_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}, \end{aligned}$$

其中 $\bar{x}_2 := x_2 + 1$． 因此，坐标变换序列 $\bar{x}_i := x_i + 1$ （在 $\mathbf{F}_2^m$ 中)就将上述和变成了与 $x_1x_2 + \cdots + x_{2k-1}x_{2k}$ 或者它的补(如果 $\mathbf{1}$ 这个项在线性函数中出现)等价的表达式．我们对满足

$$x_1x_2 + \cdots + x_{2k-1}x_{2k} = 1$$

的点 $\mathbf{x}$ 计数,记之为 n_k．显然，$n_k = 3n_{k-1} + (2^{2k-2} - n_{k-1})$,由此得 $n_k = 2^{2k-1} - 2^{k-1}$． 这亦可由考虑向量 $(x_1, x_3, \cdots x_{2k-1})$ 得到．如果它非零，那么 $(x_2, x_4, \cdots x_{2k})$ 的选择就有 2^{k-1} 种可能．因此,$n_k = (2^k - 1)2^{k-1}$．

4.7.11 因为 3 元 Hamming 码是自对偶的，所以 C 是自对偶的；($J-I$ 的秩为 4，因而 C 是 6 维的)．因此，C 的极小距离为 3 或 6．显然，G 的前 4 行的一个线性组合的重量 >4．另一方面，最后两行的一个线性组合的重量为 6．又由于 $J-I$ 的秩为 4，包含这两种行的线性组合不可能具有重量 3．

第五章

5.5.1. 对于所要求的码 C，我们通过依次选取列来构造一个适当的奇偶校验矩阵．任何非零列都可以作为我们的第一个选择．假设 m 列已经选好，我们选择接下去的一个列，使它不是前面任意 i 列的线性组合，$i \leqslant d-2$．这保证奇偶校验矩阵的任何 $d-1$ 列都是线性无关的，即码的极小距离至少是 d．如果从已选择的 m 列中取至多 $d-2$ 列的线性组合个数小于 q^{n-k} (对每个 $m \leqslant n-1$)，那么这个方法可以奏效的．因此，一个充分条件是

$$\sum_{i=0}^{d-2} \binom{n-1}{i}(q-1)^i < q^{n-k}.$$

(5.1.8) 的不等式左端至少是上式左端的 $n(q-1)/(d-1)$ 倍，而右端只是上式右端的 q 倍，即问题 5.1.1 是比一般情形下更强的结果．

5.5.2. 由 (5.1.3)，我们有 $A(10,5)=A(11,6)$．最优界由 (5.2.4) 可得(亦可见问题 4.7.3 的解)，我们得到一个 $(11,12,6)$ 码．因此 $A(10,5)=12$．

5.5.3. 在 (5.2.4) 中，等式成立仅当证明中所用到的不等式也是等式成立，而这又仅当 $\frac{1}{2}M^2$ 是整数才行．所以，$M=l$ 是不可能的．

5.5.4. 由问题 4.7.4，我们有 $A(17,8) \geqslant 36$．从 § 5.2 可得到的最好结果是利用 Plotkin 界所得到的估计．我们有

$$A(17,8) \leqslant 4A(15,8) \leqslant 64.$$

应用定理 5.3.4 可以得到一个好得多的结果：$A(17,8) \leqslant 50$．读

者可以验证这个结果. 已知的最好的界是 $A(17,8)\leqslant 37$, 它是通过改进(5.3.4)的方法得到的(参见[6]).

5.5.5. 生成矩阵的列是 PG(4,2) 中的点 (x_1,x_2,x_3,x_4,x_5). 我们知道这个[31,5]码的所有非零码字的重量都是 16 (参见问题 3.7.10). 由同一个结果可得对应于 $x_1=x_2=0$ 的坐标位置产生一个长为 7 的子码, 其所有非零重量都等于 4; 而对应于 $x_3=x_4=x_5=0$ 的坐标位置产生一个长为 3 的子码, 其非零重量都等于 2. 如果我们去掉这 10 个位置来删减原来的码, 那么所得的[21, 5] 码具有极小距离 $d=16-4-2=10$. 由 (5.2.6), 我们有 $n\geqslant 10+5+3+2+1=21$. 即缩短码达到了 Griesmer 界.

5.5.6. 这是引理 5.2.14 的证明的直接推论(出现一对 1 的平均次数是 $|C|\binom{w}{2}\Big/\binom{n}{2}=A(n-2,2k,w-2)$, 并且任意一对出现的次数都不超过这个数).

5.5.7. 设 $n=2^k-2$, 由引理 5.2.14, 有

$$A(n,3,3)=\frac{1}{6}n(n-1).$$

因此, 根据定理 5.2.15 就有

$$A(n,3)\leqslant 2^n\Big/\left\{1+n+\left(\binom{n}{2}-\frac{3n(n-2)}{6}\right)\Big/\binom{n}{2}\right\}=2^{n-k}.$$

所以, 这个 $[n,n-k,3]$ 缩短 Hamming 码是最优的.

5.5.8. 若重为 w 的两个码字 $\mathbf{c},\mathbf{c}'$ 的距离为 2, 比如说 $c_j=c'_k=1$, $c'_j=c_k=0$, 则

$$\sum_{i=0}^{n-1} ic_i-\sum_{i=0}^{n-1} ic'_i\equiv j-k\pmod n.$$

由此可得, 每个码 $C_l(0\leqslant l\leqslant n-1)$ 的极小距离都是 4. 故由 $\sum_{l=0}^{n-1}|C_l|=\binom{n}{w}$ 可知 $A(n,4,w)\geqslant\frac{1}{n}\cdot\binom{n}{w}$. 根据引理 5.2.14, 有 $A(n,4,w)\leqslant\binom{n}{w}\Big/(n-w+1)$. 综合这些不等式

即得结论.(这个思想的推广见[30].)

5.5.9. 设 C 是二元 $(n,M,2k)$ 码,定义

$$S:=\{(\mathbf{c},\mathbf{x})\mid \mathbf{c}\in C,\mathbf{x}\in \mathbf{F}_2^n,d(\mathbf{c},\mathbf{x})=w\}.$$

显然,$|S|=\binom{n}{w}M$. 对固定的 $\mathbf{x}$,C 中至多有 $A(n,2k,w)$ 个码字 $\mathbf{c}$ 使得 $d(\mathbf{c},\mathbf{x})=w$. 因此,$\binom{n}{w}M\leqslant 2^nA(n,2k,w)$.

5.5.10. (i) 该不等式的证明本质上与引理 5.2.10 的证明是一致的. 如果一个常重量码有 m_i 个码字在第 i 个位置为 1,则按我们通常的记法就有

$$2k\binom{M}{2}=\sum_{i=1}^{n}m_i(M-m_i)\leqslant M^2w-n\left(\frac{Mw}{n}\right)^2.$$

(ii) 设 $2k/n\to\delta$,当 $n\to\infty$. 又设 $w/n\to\omega$,当 $n\to\infty$,则 $A(n,2k,w)$ 当 $n\to\infty$时有界, 并且由问题 5.5.9 得 $\alpha(\delta)\leqslant 1-H_2(\omega)$. 同时还必然满足 $1-(w/k)(1-(w/n))>0$. 所以当 $1-(2\omega/\delta)(1-\omega)=0$,即 $\omega=\frac{1}{2}-\frac{1}{2}\sqrt{1-2\delta}$ 时, 就可得最佳结果,这就是(5.2.12).

5.5.11. 我们有

$$K_2(i)=2i^2-2ni-\binom{n}{2}<2d^2-2nd+\binom{n}{2},$$

对 $0\leqslant i\leqslant n-d$. 因为 $A_0=A_n=1$ (不失一般性), 且当 i 在 $[d,n-d]$ 之外时 $A_i=0$,由(5.3.3)我们就得到

$$2\binom{n}{2}+\left(2d^2-2nd+\binom{n}{2}\right)\sum_{i=d}^{n-d}A_i\geqslant 0.$$

由此即得所要的不等式.

5.5.12. 考虑由定理 5.3.4 来确定 $A(9,4)$. 我们有关于 A_4,A_6,A_8 的 4 个不等式, 再加上一个明显的不等式 $A_8\leqslant 1$. 经过相当冗长的计算,可以得到最优解 $A_4+A_6+A_8\leqslant 20\frac{1}{3}$. 因此,我们

需要考虑存在(9,21,4)码的可能性。 在引理 5.3.3 的证明中，取 $\omega = -1$,得到不等式

$$21\sum_{i=0}^{9}A_iK_k(i)\geqslant\binom{9}{k},$$

即

$$\frac{20}{21}K_k(0)+\sum_{i=1}^{9}A_iK_k(i)\geqslant 0,$$

这里用到 $K_k(0)=\binom{9}{k}$. 因为该码有 21 个码字，所以至多有 10 对码字,其每对的距离为 8, 即 $A_8\leqslant\frac{20}{21}$. 所以 $\frac{21}{20}A_i$ 必定满足开始时解得的不等式. 这意味着

$$A_4+A_6+A_8\leqslant\frac{20}{21}\cdot\frac{61}{3}<20.$$

矛盾.

第六章

6.11.1. 我们将 § 6.1 和 § 6.2 加以推广. 在 $\mathbf{F}_3$ 上有

$$x^4+1=(x^2+x+2)(x^2+2x+2).$$

因此, x^2+x+2 是一个负循环[4,2]码的生成元,该码的生成矩阵为$\begin{pmatrix}2&1&1&0\\0&2&1&1\end{pmatrix}$. 由定义 3.3.1,这是一个[4,2] Hamming 码.

6.11.2. 由于 x^4+x+1 是本原多项式，故可取之为[15,11] Hamming 码的生成元. 利用证明定理 6.4.1 的方法,求得

$$a(x)(x^4+x+1)=1+(x+x^2+x^4+x^8)$$
$$+(x^3+x^6+x^9+x^{12}),$$

这是与三个分圆陪集相对应的幂等元之和. 定理 6.4.4 之后叙述的方法及例子提供了第二种解法.

6.11.3. 考虑 § 4.5 中引进的矩阵 E，删去第一列,我们便得到了 AG$(m,2)$ 中所有 $\neq(0,\cdots,0)$的点(写成列向量). 也可以把

这些点看作 $\mathbf{F}_{2^m}^*$ 的元素，它是一个由 $\mathbf{F}_{2^m}^*$ 的本原元 ξ 生成的乘法群. 由 $A(x):=\xi x$ 所定义的 $\mathbf{F}_{2^m}$ 到 $\mathbf{F}_{2^m}$ 的映射 A 显然是 $\mathrm{AG}(m,2)$ 到自身的一个非退化的线性变换，并且作为 $\mathrm{AG}(m,2)\backslash\{\mathbf{0}\}$ 的点的置换是 2^m-1 阶的. 映射 A 把平坦映到平坦. 于是由引理 4.5.5(i)，4.5.6 以及定理 4.5.9 知，与 A 对应的坐标位置的置换可导出缩短 Reed-Muller 码的一个循环表示.

6.11.4. 由 x^3+2x+1 生成 $\mathbf{F}_3^3$. 如果 β 是一个本原元，x^3+2x+1 是其极小多项式，利用域的运算表就能得到 β^2 的极小多项式为 $(x-\beta^2)(x-\beta^6)(x-\beta^{18})=x^3+x^2+2$，$\beta^4$ 的极小多项式为 x^3+2x+2. 这些多项式的积是一个包含 $\beta,\beta^2,\beta^3,\beta^4$ 为零点的多项式. 因此它生成所求的码. 即该码的生成多项式是 $1+x+x^2+x^3+2x^4+x^6+2x^7+x^9$，码是 17 维的.

6.11.5. 首先作 $\mathbf{F}_{2^5}$ 的表. 经过替换，我们发现对 $i=1,2,3,4$ 有 $E(\alpha^i)=R(\alpha^i)$，它们分别是 $\alpha^{28},\alpha^{25},1,\alpha^{19}$. 我们必须由方程 $1+\sigma_1\alpha^{25}+\sigma_2\alpha^{28}=0$ 和 $\alpha^{19}+\sigma_1+\sigma_2\alpha^{25}=0$ 来确定 $\sigma(z)=1+\sigma_1 z+\sigma_2 z^2$. 可以求得 $\sigma_1=\alpha^{28}$，$\sigma_2=\alpha^{10}$，即

$$\sigma(z)=(1-\alpha^{14}z)(1-\alpha^{27}z).$$

由此，码字为

$$(10010\ 11011\ 11001\ 01101\ 01010\ 11011\ 1),$$

码的生成多项式是 $(1+x^2+x^5)(1+x^2+x^3+x^4+x^5)$，即 $g(x)=1+x^3+x^5+x^6+x^8+x^9+x^{10}$，码字为

$$g(x)(1+x^{11}+x^{20}).$$

6.11.6. 我们先对 $l=-2,c_1=3,c_2=1,d_0=3,s=1$ 应用定理 6.6.3，求得 $d\geqslant 4$. 考察 C 的偶重量子码 C'，该码的码字以 $\beta^{-2},\beta^{-1},\beta^0,\beta^1,\beta^2$ 为零点. 因此，由 BCH 界得 C' 的极小距离至少为 6. 故有 $d\geqslant 5$.

6.11.7. 考察任意一个 $[q+1,2,q]$ 码 C'. 这个码在任意两个位置上是系统的(见(3.7.2)). 这表明，重量计数子的系数满足

$$(q+1)A_{q+1}+qAq=(q+1)(q^2-q).$$

因为 $A_{q+1}+A_q=q^2-1$，所以，$A_{q+1}=0$，即每个非零码字的重

量为 q. 存在唯一的码字 $\mathbf{c}=(c_0, c_1, \cdots, c_q)$ 满足 $c_0=c_{(q+1)/2}=1$. 由于 $\mathbf{c}$ 恰有一个坐标是 0,所以 $\mathbf{c}$ 在 $\frac{1}{2}(q+1)$ 个位置上的一个循环移位不会得到同一个码字. 因此, C' 不是循环码.

6.11.8. 在 $\mathbf{F}_3$ 上我们有:

$$x^{11}-1=(x-1)(x^5-x^3+x^2-x-1)(x^5+x^4-x^3+x^2-1),$$

其中的因子都是不可约的. 因此,如在(6.9.1)中那样,我们可以取 $g_0(x)=(x^5-x^3+x^2-x-1)$ 作为三元 [11,6] QR 码 C 的生成多项式. 由 BCH 界和定理 6.9.2,都能得到 $d \geqslant 4$, 后一种情形限制 $c(1) \neq 0$. 码 $C^{\perp}$ 的生成多项式为 $(x-1)g_0(x)$(见 § 6.2). 现在考察按通常方式加上奇偶校验位所得的码 $\bar{C}$. 如果 G 是 $C^{\perp}$ 的一个生成矩阵, 那么 G 添上行 $\mathbf{1}$ 就可得到 C 的生成矩阵, 而 $\bar{C}$ 的生成矩阵是

$$\left[\begin{array}{ccc|c} & & & 0 \\ & G & & 0 \\ & & & \vdots \\ & & & 0 \\ \hline 1 & 1 \cdots & 1 & 1 \end{array}\right].$$

我们看到 $\bar{C}$ 是自对偶的. 一个码字与其自身的内积(在 $\mathbf{R}$ 上的)是它的非零坐标的个数. 因此, $\bar{C}$ 的每个码字的重量都是 3 的倍数,这表明 $d \geqslant 5$. 利用 $1+\binom{11}{1}2+\binom{11}{2}2^2=3^5$ 及定义, 可知 C 是完全的.

6.11.9. 由(6.9.5), d 是奇数. 又由定理 6.9.2(ii) 和 (iii), 可得 $d^2-d+1 \geqslant 47$ (即 $d \geqslant 8$) 以及 $d \equiv 3 \pmod 4$. 因此, $d \geqslant 11$. 由 Hamming 界(定理 5.2.7),我们有

$$\sum_{i=0}^{e}\binom{47}{i} \leqslant 2^{47}/|C|,$$

其中, $d=2e+1$. 因为 C 是 24 维的, 所以 $e \leqslant 5$. 由此即得

$d = 11$.

6.11.10. 在 § 6.9 的例题和问题 6.11.8中，我们已经有一个[7, 4] Hamming 码和两个 Golay 码作为完全 QR 码的例子. 还有另一个完全 QR 码的例子. 作为第七章的结果的推论，对于 $e > 1$,没有其它的完全 QR 码. 设 C 是 $\mathbf{F}_q$ 上长为 n 的一个 QR 码，再设它是极小距离 $d = 3$ 的完全码，则由(3.1.6)有

$$1 + n(q-1) = q^{(n-1)/2},$$

因此，

$$n = 1 + q + q^2 + \cdots + q^{(n-3)/2}.$$

如果 $n > 5$,则上式右端至少为

$$1 + 2 + \frac{n-5}{2} \cdot 4 = 2n - 7,$$

即 $n = 7, q = 2$. 这时 C 是 [7,4] Hammirg 码. 剩下的是讨论 $n = 3$ 和 $n = 5$ 的情形. 我们分别有

$$1 + 3(q-1) = q \text{ 和 } 1 + 5(q-1) = q^2.$$

因此,唯一的解是 $n = 5, q = 4$.

6.11.11. 设 β 是 $\mathbf{F}_n$ 的一个本原元, 定义 $B_\nu: = \{\beta^i \in \mathbf{F}_n | i \equiv \nu \pmod{e}\}, 0 \leqslant \nu \leqslant e$. 设 α 是 $\mathbf{F}_q$ 的扩域中的一个 n 次本原单位根,定义

$$g_\nu(x): = \prod_{r \in k_\nu} (x - \alpha^r), 0 \leqslant \nu \leqslant e.$$

因为 $q \in R_0$,所以每个 g_ν 的系数都在 $\mathbf{F}_q$ 中. 进一步, 这些多项式都是 $(n-1)/e$ 次的,而且

$$x^n - 1 = (x-1)g_0(x)g_1(x)\cdots g_{e-1}(x).$$

e 次幂剩余码 C 的生成多项式是 $g_0(x)$,它与以 $g_\nu(x)$ 为生成多项式的码等价.仿照定理 6.9.2(i) 的证明可得 $d^e > n$. 如果 $n = 31$, $e = 3, q = 2$, 那么可得 $d^3 > 31$, 即 $d \geqslant 4$. 由于在 $\mathbf{F}_{31}$ 中 $5^3 = -1$,我们得到 $g_0(\alpha) = g_0(\alpha^{-1}) = 0$. 因此,根据问题 6.11.6 就有 $d \geqslant 5$. 进一步,由 Hamming 界,必有 $d < 7$. 事实上, Hamming 界还保证由码 C 中的具有奇重量的 2^{20} 个码字所组成的码不可能

有 $d=6$. 因此, $d=5$.

6.11.2. (a) 因为 $\alpha,\alpha^2,\alpha^4,\alpha^5$ 是码字的零点,所以, $d\geqslant 4$ 是定理 6.6.3 的一个直接推论.

(b) 由 BCH 界, $d\geqslant 3$. 若 $d=3$,则存在一个码字, 它在 0, i, j 这三个位置取值为 1. 令 $\xi=\alpha^i$, $\eta=\alpha^j$, 则 $1+\xi+\eta=0$, $1+\xi^5+\eta^5=0$. 于是,

$$1=(\xi+\eta)^5=(\xi^5+\eta^5)+\xi\eta(\xi^3+\eta^3),$$

即 $\xi^3+\eta^3=0$. 矛盾,因为 $2^m-1\not\equiv 0(\mathrm{mod} 3)$, 所以 $x^3=1$ 只有唯一解 $x=1$,然而 $\xi\neq\eta$.

6.11.13. 考察 6.11.8 中的表示. 设 α 是 $\mathbf{F}_{3^5}$ 的一个本原元, 则 α^{22} 是 11 次本原单位根, 即为 $g_0(x)$ 或 $g_1(x)$ 的一个零点. 因此, $1,\alpha^{22},\alpha^{44},\cdots,\alpha^{220}$ 作为 $(\mathbf{F}_3)^5$ 的元素的表示是 C 的奇偶校验矩阵的列. 用 $-1=\alpha^{121}$ 乘 $\alpha^{22i}(i>5)$ 所对应的列, 经重排我们得到 $1,\alpha^{11},\alpha^{22},\cdots,\alpha^{110}$, 它们对应于 $x^{11}+1$ 的零点. 这个码等价于 C (而又知 C 是唯一的),并且这个表示是负循环的.

第七章

7.7.1. 设 C 是这个码. 因为长为 $n+1=2^m-1$ 的 Hamming 码是 $e=1$ 的完全码, 所以, C 的覆盖半径为 2. 在(5.2.16)中置 $n=2^m-2$, $|C|=2^{n-m}$, $e=1$, 就得到了等式. 因此, C 是负完全码.

7.7.2. 假设 $\rho(\mathbf{u},C)=2$,即 $\mathbf{u}=\mathbf{c}+\mathbf{e}$,其中 $\mathbf{c}\in C$, $\mathbf{e}$ 的重量为 2. 于是, $c(\alpha)=c(\alpha^3)=0$,并且, $e(x)=x^i+x^j$, 对某个 i,j. 我们现在计算有多少种方法可以用来改变三个位置 (记为 x_1,x_2,x_3),从而求出一个码字. 因此,我们就要计算

$$x_1+x_2+x_3+\alpha^i+\alpha^j=0,$$
$$x_1^3+x_2^3+x_3^3+\alpha^{3i}+\alpha^{3j}=0$$

的解的个数. 作替换 $y_i:=x_i+e(\alpha)$,我们发现

$$y_1+y_2+y_3=0,$$
$$y_1^3+y_2^3+y_3^3=s:=\alpha^{i+j}(\alpha^i+\alpha^j),$$

其中 $s \neq 0, y_k \notin \{\alpha^i, \alpha^j\}$.

由第一个方程，我们有 $y_3 = y_1 + y_2$. 将其代入第二个方程，得到

$$y_1 y_2 (y_1 + y_2) = s.$$

由于 $s \neq 0$,有 $y_2 \neq 0$. 令 $y := y_1/y_2$, 则方程变形为

$$y(1 + y) = s/y_2^3.$$

因为 $(3, n) = (3, 3^{2m+1} - 1) = 1$,所以对于 y 的除 0,1 之外的每个值,方程(在 $F_{2^{2m}}$ 中)有唯一解 y_2. 因此，我们求得 $n - 1$ 个解 $\{y_1, y_2\}$, 从而亦可得 y_3. 显然,每个三元组都出现 6 次,并且必须去掉 $y_1 = \alpha^i, y_2 = \alpha^j$ 这个解,因为它们对应于 $x_1 = \alpha^j$, $x_2 = \alpha^i$, $x_3 = 0$ (或者它们的任何一个置换). 因此，$\rho(\mathbf{u}, C) = 2$ 意味着有 $\frac{1}{6}(n - 1) - 1$ 个与 $\mathbf{u}$ 距离为 3 的码字. 用类似的方法可以讨论 $\rho(\mathbf{u}, C) > 2$ 的情形.

7.7.3. 码 C 是长为 15 的 Preparata 码. 然而，我们无需利用这个事实. 由(16,256,6) Nordstrom-Robinson 码 $\bar{C}$ 入手，删减后得到一个(15,256,6)码 C. 这些参数使(5.2.16)成立.

7.7.4. 易见,码 C 不等价于线性码. 否则，$0 \in C$, C 就是一个线性码. 因而 C 的任两个码字之和仍属于 C. 但这显然不成立. 为了证明 C 是完全的,我们需要考察码字 $\mathbf{a} = (\mathbf{x}, \mathbf{x} + \mathbf{c}, \sum x_i + f(\mathbf{c}))$ 和 $\mathbf{b} = (\mathbf{y}, \mathbf{y} + \mathbf{c}', \sum y_i + f(\mathbf{c}'))$. 若 $\mathbf{c} = \mathbf{c}'$, $\mathbf{x} \neq \mathbf{y}$, 则显然有 $d(\mathbf{a}, \mathbf{b}) \geqslant 3$. 如果 $\mathbf{c} \neq \mathbf{c}'$, 则 $d(\mathbf{a}, \mathbf{b}) \geqslant w(\mathbf{x} - \mathbf{y}) + w(\mathbf{x} + \mathbf{c} - \mathbf{y} - \mathbf{c}') \geqslant w(\mathbf{c} - \mathbf{c}') \geqslant 3$. 由于 $|C| = 2^{11}$ 且 $d = 3$,所以(3.1.6)中的等号成立. 即 C 为完全码.

7.7.5. 设 x_1, x_2 是 Ψ_2 的两个零点,则由(7.5.2)及(7.5.6)可得

$$x_1 + x_2 = n + 1 \text{ 以及 } x_1 x_2 = 2^{l-1}.$$

因此，$x_1 = 2^a, x_2 = 2^b (a < b)$. 由(3.1.6)可得 $n^2 + n + 2 = 2^c$ (这里,由于 $n \geqslant 2$, 有 $c \geqslant 3$).

故有

$$(2^a + 2^b)(2^a + 2^b - 1) + 2 = 2^c.$$

但是左端有一项为 2，因此另一项不能被 4 整除. 所以，$a=0$ 或者 $a=1$. 如果 $a=0$，则有 $2^b(2^b+1)+2=2^c$，即 $b=1$，$n=2$. 相应的码是 $C=\{(0,0)\}$. 如果 $a=1$，则 $2^{2b}+3\cdot 2^b+4=2^c$，即 $b=2$，$n=5$，它对应着重复码 $C=\{(00000),(11111)\}$.

7.7.6. 首先应用定理 7.3.5 和(1.2.7)，我们得到方程

$$4x^2-4(n+1)x+(n^2+n+12)=0,$$

其解为 $x_{1,2}=\frac{1}{2}(n+1\pm\sqrt{n-11})$.

这意味着对某个整数 m，有 $n-11=m^2$. 由(7.3.6)有

$$\begin{aligned}12\cdot 2^n &= |C|\cdot(n^2+n+12)\\ &= |C|(n+1+m)(n+1-m),\end{aligned}$$

故 $n+1+m=a\cdot 2^{\alpha+1}$，$n+1-m=b\cdot 2^{\beta+1}$，这里 $ab=1$ 或 3. 先设 $a=b=1$. 这时，$n+1=2^\alpha+2^\beta$，$m=2^\alpha-2^\beta(\alpha>\beta)$. 因此，有

$$2^\alpha+2^\beta-12=2^{2\alpha}-2^{\alpha+\beta+1}-2^{2\beta},$$

即

$$-12=2^\alpha(2^\alpha-2^{\beta+1}-1)+2^\beta(2^\beta-1),$$

这显然是矛盾的.

下设 $b=3$. 于是 $n+1=a\cdot 2^\alpha+3\cdot 2^\beta$，$m=a\cdot 2^\alpha-3\cdot 2^\beta$. 因此

$$3\cdot 2^\beta(3\cdot 2^\beta-2^{\alpha+1}-1)+2^\alpha(2^\alpha-1)+12=0.$$

如果 $\alpha>2$，则必有 $\beta=2$，因而 $\alpha=4$. 由于 $\alpha\leqslant 2$ 时无解，且在最后的情形 $a=3$ 也得不到任何结果，因此我们证明了 $n+1=2^4+3\cdot 2^2$，即 $n=27$.

这种码的构造方法类似于(7.4.2). 由

$$x_1x_2+x_3x_4+x_5x_6+x_5+x_6=0$$

替换(7.4.2)中的形式，其余的论证都一样. 我们求得了一个长为 27 的双重量码，其码字的重量为 12 或者 16，这样再应用定理 7.3.7 即得.

第八章

8.8.1. 在定理 8.3.1 中，我们证明了用 $\hat{g}(z) := z + 1$ 替换 $g(z)$ 能得到同一个码. 因此，$\Gamma(L, g)$ 至少是 4 维的，并且其极小距离 $d \geqslant 3$. 正如在 § 8.3 的第一部分所证明的，d 可能会更大一些. 我们构造奇偶校验矩阵 $H = (h_0, h_1, \cdots h_7)$，这里 h_j 取遍使 $(j, 15) = 1$ 的所有 $(\alpha^j + 1)^{-1}$ 的值. 注意到 H 由所有最后一个分量为 1 的向量组成，即 $\Gamma(L, g)$ 是扩充[8,4,4] Hamming 码.

8.8.2. 设 $\mathbf{a}$ 是 C 中的一个偶重量字. 由 (6.5.2)，相应的 Mattson-Solomon 多项式 $A(X)$ 能被 X 整除. 根据定理 8.6.1，$g(X)$ 能整除 $X^{n-1} \circ A(X)$，即 $X^{-1}A(X)$. 由于 C 是循环码，由 (6.5.2)知 $g(\alpha^i X)$ 亦能整除 $X^{-1}A(X)$，对于 $0 < i \leqslant n - 1$. 如果 $g(X)$ 在 $\mathbf{F}_2$ 的任何扩域中有异于 0 的零点，则 $X^{-1}A(X)$ 有 $n - 1$ 个互异根. 这与 $\deg X^{-1}A(X) < n - 1$ 矛盾. 因此，有 t 使 $g(z) = z^t$，从而 C 是 BCH 码(参见(8.2.6)).

8.8.3. 这恰好就是 § 8.3 第一部分所证明的. 对任一个码字 $(b_0, b_1, \cdots, b_{n-1})$，我们有 $\sum_{i=0}^{n-1} b_i \gamma_i^r = 0$，$0 \leqslant r \leqslant d_1 - 2$，这里，$\gamma_i = \alpha^i$ (α 是一个本原元). 因此，极小距离

$$\geqslant (d_2 - 1) + (d_1 - 2) + 2 = d_1 + d_2 - 1.$$

8.8.4. 用 $G^{-1}(X)$ 表示 $G(X)$ 在环 $(T, +, \circ)$ 中的逆元. GBCH 码的定义可以叙述为

$$P(X) \cdot (\Phi a)(X) = Q(X)G(X) + R(X)(X^n - 1),$$

其中 $Q(X)$ 的次数 $< n - t$. 这等价于

$$(G^{-1}(X) \circ P(X)) \cdot (\Phi a)(X) = Q(X) + R^*(X)(X^n - 1),$$

对某个适当的 $R^*(X)$. 如果取偶 $(\hat{P}(X), X^t)$，这里

$$\hat{P}(X) = X^t \circ G^{-1}(X) \circ P(X),$$

我们可以得到同样的条件，包括要求 $\deg Q(X) < n - t$.

8.8.5. 在(6.6.1)中取 $l = 5, \delta = 2$，我们知 C 是 BCH 码，其极

小距离 $d \geqslant 2$. 因为 $(x+1)(x^2+x+1)=x^3+1\in C$，所以 $d=2$. 若在(8.2.4)中取 $g(x)$ 的次数>1，则由定理 8.2.7，Goppa 码 $\Gamma(L,g)$ 的极小距离至少为 3. 如果 $g(x)$ 是 1 次的，则由定理 8.3.1 能得到同样的结论. 所以 C 不是 Goppa 码.

第九章

9.4.1. C_α 的码字具有形式 $(a(x),\ \alpha(x)a(x))$，这里 $a(x)$ 和 $\alpha(x)$ 都是模 x^6+x^3+1 的多项式. 为了使 $d>3$，我们必须排除这样的 $\alpha(x)$：当 $a(x)=x^i$ 时，$\alpha(x)a(x)=x^j+x^k$. 同时也将这些 $\alpha(x)$ 的逆排除. 由 $(1+x)^8=1+x^8=x^{-1}(x+x^9)=x^{-1}(x+1)$，易见 $\mathbf{F}_{2^6}$ 中的每个元都可唯一地表成 $x^i(1+x^j)$，其中

$$i\in\{0,\pm1,\pm2,\pm3,\pm4\},\ j\in\{0,\pm1,\pm2,\pm4\}.$$

于是，$d>2$ 就排除了 9 个 $\alpha(x)$，$d>3$ 就排除了余下的 54 个 $\alpha(x)$. 这表明对于较小的 n，所给的构造方法并不怎么好. 由(3.7.14)，存在一个扩充的(12,7]字典序最小码，其极小距离 $d=4$. 在(4.7.3)中，我们看到存在 $n=12$，$d=4$ 的非线性码，它含有更多的码字.

9.4.2. 设 $\alpha(x)$ 是重为 3 的多项式，则 $(a(x),\alpha(x)a(x))$ 的两部分的重量具有相同的奇偶性. 所以，仅当有一种选择 $a(x)=x^i+x^j$ 使 $\alpha(x)a(x)\equiv 0\ (\mathrm{mod}\,x^6-1)$ 时，才可能 $d<4$. 而这种情形只在 $\alpha(x)$ 是周期的，即为 $1+x^2+x^4$ 或 $x+x^3+x^5$ 时才出现. 对所有其它选择，都有 $d=4$.

9.4.3. 设信息率 R 满足 $\dfrac{1}{l+1}<R\leqslant\dfrac{1}{l}\ (l\in\mathrm{N})$. 又设 s 是使 $m/[(l+1)m-s]\geqslant R$ 的最小整数. 按下述方法构造一个码 C：选取一个 l 元组 $(\alpha_1,\alpha_2\cdots,\alpha_l)\in(\mathbf{F}_{2^m})^l$，再对所有的 $\mathbf{a}\in\mathbf{F}_2^m$ 构造 $(\mathbf{a},\alpha_1\mathbf{a},\cdots,\alpha_l\mathbf{a})$，最后去掉后面的 s 个符号. 从而字长 $n=(l+1)m-s$.

一个非零字 $c\in C$ 对应着 2^s 个可能的 l 元组 $(\alpha_1,\cdots,\alpha_l)$.

为了保证极小距离$\geqslant \lambda n$,至多要排除 $2^s \sum_{i<\lambda n}\binom{n}{i}$个$(\alpha_1,\cdots,\alpha_l)$ 的值。如果还能选择到 $(\alpha_1,\cdots,\alpha_l)$,即若

$$2^s \sum_{i<\lambda n}\binom{n}{i} < 2^{ml},$$

则条件得到满足。由定理 1.4.5,我们有

$$s + nH(\lambda) < ml,$$

即

$$H(\lambda) < \frac{ml-s}{n} = 1 - \frac{m}{n} = 1 - R + o(1), \quad (m \to \infty).$$

第十章

10.5.1. 考察序列 $r, r^2, r^3, \cdots$, 其中必有两个元素模A同余,比如说 $r^n - r^m \equiv 0(\mathrm{mod} A)\ (n > m)$.

10.5.2. 设 $m = r^n - 1 = AB$, 其中 $A > r^2$ 为素数。 又设 r 生成 $\mathbf{F}_A^*$ 的一个子群 H, 且 $|H| = n$, 则 $\{\pm c | c = 1, 2, \cdots, r-1\}$ 是它的一个完全的陪集代表系。考虑基为 r, 长为 n 的循环 AN 码 C。显然,区间 $[1, m]$ 中的每个整数都恰与C的一个码字的模距离为 0 或1. 因此,C 是完全码.(因为 $w_m(A) \geqslant 3$, 故必有 $A > r^2$.) 当 $r = 3$ 时,一个平凡的例子就是循环码 $\{13, 26\}$,这里,我们取 $m = 3^3 - 1, A = 13$.

$\mathbf{F}_{13}^*$ 的由 3 生成的子群指标为 4,陪集代表元为± 1 和± 2.

10.5.3. 我们有 $455 = \sum_{i=0}^{5} b_i 3^i$,其中 $(b_0, b_1, \cdots, b_5) = (2, 1, 2, 1, 2, 1)$. 根据(10.2.3)中描述的算法,以$-1, 2$ 代替初始值 $2, 1$. 用这种方法,我们得到下述的表示序列:

$$\begin{aligned}(2,1,2,1,2,1) &\longrightarrow (-1,2,2,1,2,1) \longrightarrow (-1,-1,0,2,1,1)\\ &\longrightarrow (-1,-1,0,-1,0,2)\\ &\longrightarrow (0,-1,0,-1,0,-1).\end{aligned}$$

因此,在 CNAF 中的表示是

$$455 \equiv -273 \equiv -3-3^3-3^5.$$

10.5.4. 我们验证定理 10.3.2 的条件. 在 $\mathbf{F}_{11}^{*}$ 中,元素 3 生成子群$\{1,3,9,5,4\}$,分别乘以-1就得到其余的 5 个元素. $r^n=3^5=243=1+11\cdot 22$. 所以,$A=22$,其 3 元表示为 $A=1+1\cdot 3+2\cdot 3^2$. 22 的 CNAF 是 $1-2\cdot 3+0\cdot 3^2+1\cdot 3^3+0\cdot 3^4 \pmod{242}$. 码含有 10 个码字，它们分别是 $(1,-2,0,1,0)$ 和 $(-1,2,0,-1,0)$ 的循环移位，每个字的重量都是 3.

第十一章

11.7.1. 利用 §11.1 的符号,我们有

$$G(x)=(1+(x^2)^2)+x(1+x^2)=1+x+x^3+x^4.$$

信息流 11111$\cdots$给出了 $I_0(x)=(1+x)^{-1}$,因而有

$$T(x)=(1+x^2)^{-1}G(x)=1+x+x^2,$$

即接收流为 1110000$\cdots$.

最初三个位置发生错误时,使接收流成为全 0 流,从而导致无穷多个译码错误.

11.7.2. 在定理 11.4.2 中我们证明了怎样才能出现这种情况. 设 $h(x)=x^4+x+1$, $g(x)h(x)=x^{15}-1$. 我们知道 $g(x)$ 生成一个极小距离为 8 的不可约循环码. 考虑信息序列 110010000$\cdots$, 即 $I_0(x)=h(x)$,则有

$$T(x)=h(x^2)g(x)=(x^{15}-1)h(x),$$

其重量为 6,由定理 11.4.2, 这就是自由距离. 在该例中, $g(x)=x^{11}+x^8+x^7+x^5+x^3+x^2+x+1$. 因此 $G_0(x)=1+x+x^4$, $G_1(x)=1+x+x^2+x^3+x^5$. 编码器见图 8.

而

$$I_0=11001000\cdots,$$

输出为

$$T=11001\ 00000\ 00000\ 11001\ 0000\cdots.$$

11.7.3. 考虑任一非零输出序列. 显然, 初始的 7 元组是由 m_3 生成的循环码中的一个非零码字, 故其重量≥ 3. 类似地,输出中最后一个非零 7 元组是由 m_0m_1 生成的循环码的码字, 它非零, 故

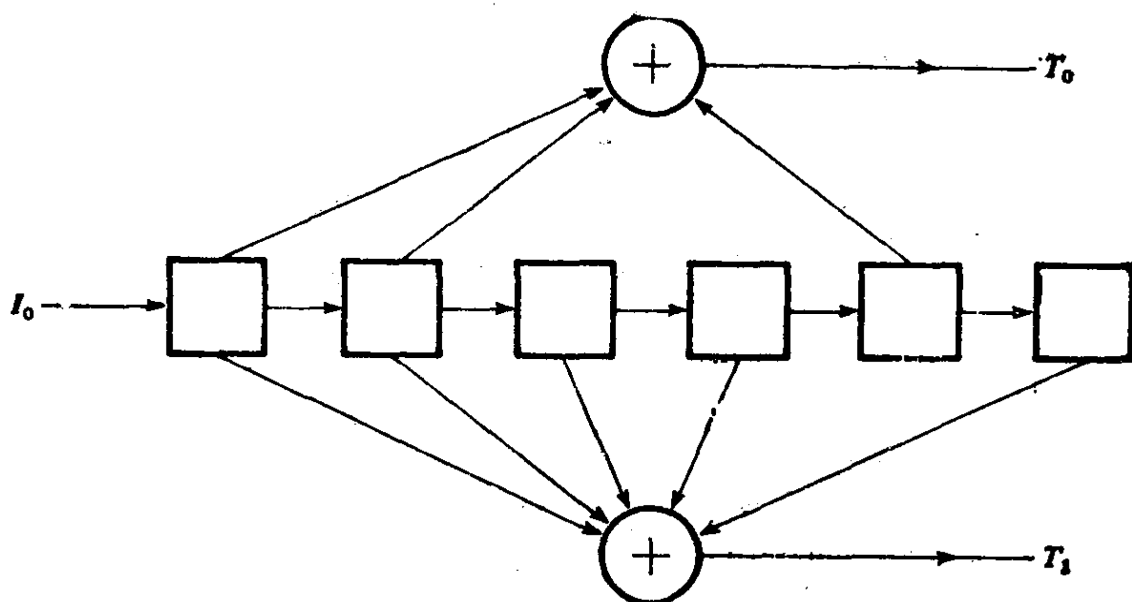


图 8

其重量≥4. 现设 $t=0$ 时的输入为 4 元组(1100),而连下去都是 0,则输出是(1100) G,即 $(m_1m_3+m_0m_3)+(m_0^3m_1)x$. 由(11.5.6)中 G 的前两行，我们看到这个输出序列是 0001011，之后紧接着 1001011,然后全是零. 故自由距离是 7.

参考文献

1. Baumert, L. D. and McEliece, R. J.: *A Golay-Viterbi Concatenated Coding Scheme for MJS '77*. JPL Technical Report 32-1526, pp. 76-83. Pasadena, Calif.: Jet Propulsion Laboratory, 1973.
2. Berlekamp, E. R.: *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
3. Berlekamp, E. R.: *Decoding the Golay Code*. JPL Technical Report 32-1256, Vol. IX, pp. 81-85. Pasadena, Calif.: Jet Propulsion Laboratory, 1972.
4. Berlekamp, E. R.: Goppa codes. *IEEE Trans. Info. Theory*, **19**, pp. 590-592 (1973).
5. Berlekamp, E. R. and Moreno, O.: Extended double-error-correcting binary Goppa codes are cyclic. *IEEE Trans. Info. Theory*, **19**, pp. 817-818 (1973).
6. Best, M. R., Brouwer, A. E., MacWilliams, F. J., Odlyzko, A. M. and Sloane, N. J. A.: Bounds for binary codes of length less than 25. *IEEE Trans. Info. Theory*, **23**, pp. 81-93 (1977).
7. Best, M. R.: *On the Existence of Perfect Codes*. Report ZN 82/78. Amsterdam: Mathematical Centre, 1978.
8. Best, M. R.: Binary codes with a minimum distance of four. *IEEE Trans. Info. Theory*, **26**, pp. 738-742 (1980).
9. Bussey, W. H.: Galois field tables for $p^n \leq 169$. *Bull. Amer. Math. Soc.*, **12**, pp. 22-38 (1905).
10. Bussey, W. H.: Tables of Galois fields of order less than 1,000. *Bull. Amer. Math. Soc.*, **16**, pp. 188-206 (1910).
11. Cameron, P. J. and van Lint, J. H.: *Graphs, Codes and Designs*. London Math. Soc. Lecture Note Series, Vol. 43. Cambridge: Cambridge Univ. Press, 1980.
12. Chen, C. L., Chien, R. T. and Liu, C. K.: On the binary representation form of certain integers. *SIAM J. Appl. Math.*, **26**, pp. 285-293 (1974).
13. Chien, R. T. and Choy, D. M.: Algebraic generalization of BCH-Goppa-Helgert codes. *IEEE Trans. Info. Theory*, **21**, pp. 70-79 (1975).
14. Clark, W. E. and Liang, J. J.: On arithmetic weight for a general radix representation of integers. *IEEE Trans. Info. Theory*, **19**, pp. 823-826 (1973).
15. Clark, W. E. and Liang, J. J.: On modular weight and cyclic nonadjacent forms for arithmetic codes. *IEEE Trans. Info. Theory*, **20**, pp. 767-770 (1974).
16. Curtis, C. W. and Reiner, I.: *Representation Theory of Finite Groups and Associative Algebras*. New York-London: Interscience, 1962.
17. Cvetković, D. M. and van Lint, J. H.: An elementary proof of Lloyd's theorem. *Proc. Kon. Ned. Akad. v. Wetensch.* (A), **80**, pp. 6-10 (1977).
18. Delsarte, P.: An algebraic approach to coding theory. *Philips Research Reports Supplements*, **10** (1973).
19. Delasarte, P. and Goethals, J.-M.: Unrestricted codes with the Golay parameters are unique. *Discrete Math.*, **12**, pp. 211-224 (1975).
20. Elias, P.: *Coding for Noisy Channels*. IRE Conv. Record, part 4, pp. 37-46.
21. Feller, W.: *An Introduction to Probability Theory and Its Applications*, Vol. I. New York-London: Wiley, 1950.
22. Forney, G. D.: *Concatenated Codes*. Cambridge, Mass.: MIT Press, 1966.

23. Forney, G. D.: Convolutional codes I: algebraic structure. *IEEE Trans. Info. Theory*, **16**, pp. 720–738 (1970); *Ibid.*, **17**, 360 (1971).
24. Gallagher, R. G.: *Information Theory and Reliable Communication*. New York: Wiley, 1968.
25. Goethals, J.-M. and van Tilborg, H. C. A.: Uniformly packed codes. *Philips Research Reports*, **30**, pp. 9–36 (1975).
26. Goethals, J.-M.: The extended Nadler code is unique. *IEEE Trans. Info. Theory*, **23**, pp. 132–135 (1977).
27. Goppa, V. D.: A new class of linear error-correcting codes. *Problems of Info. Transmission*, **6**, pp. 207–212 (1970).
28. Goto, M.: A note on perfect decimal AN codes. *Info. and Control*, **29**, pp. 385–387 (1975).
29. Goto, M. and Fukumara, T.: Perfect nonbinary AN codes with distance three. *Info. and Control*, **27**, pp. 336–348 (1975).
30. Graham, R. L. and Sloane, N. J. A.: Lower bounds for constant weight codes. *IEEE Trans. Info. Theory*, **26**, pp. 37–40 (1980).
31. Gritsenko, V. M.: Nonbinary arithmetic correcting codes. *Problems of Info. Transmission*, **5**, pp. 15–22 (1969).
32. Hall, M.: *Combinatorial Theory*. New York–London–Sydney–Toronto: Wiley (second printing), 1980.
33. Hartmann, C. R. P. and Tzeng, K. K.: Generalizations of the BCH bound. *Info. and Control*, **20**, pp. 489–498 (1972).
34. Helgert, H. J. and Stinaff, R. D.: Minimum distance bounds for binary linear codes. *IEEE Trans. Info. Theory*, **19**, pp. 344–356 (1973).
35. Helgert, H. J.: Alternant codes. *Info. and Control*, **26**, pp. 369–380 (1974).
36. Jackson, D.: *Fourier Series and Orthogonal Polynomials*. Carus Math. Monographs, Vol. 6. Math. Assoc. of America, 1941.
37. Justesen, J.: A class of constructive asymptotically good algebraic codes. *IEEE Trans. Info. Theory*, **18**, pp. 652–656 (1972).
38. Justesen, J.: An algebraic construction of rate $1/\nu$ convolutional codes. *IEEE Trans. Info. Theory*, **21**, 577–580 (1975).
39. Kasami, T.: An upper bound on k/n for affine invariant codes with fixed d/n. *IEEE Trans. Info. Theory*, **15**, pp. 171–176 (1969).
40. Levenshtein, V. I.: Minimum redundancy of binary error-correcting codes. *Info. and Control*, **28**, pp. 268–291 (1975).
41. van Lint, J. H.: Nonexistence theorems for perfect error-correcting-codes. In: *Computers in Algebra and Number Theory*, Vol. IV (SIAMS–AMS Proceedings) 1971.
42. van Lint, J. H.: *Coding Theory*. Springer Lecture Notes, Vol. 201, Berlin–Heidelberg–New York: Springer, 1971.
43. van Lint, J. H.: A new description of the Nadler code. *IEEE Trans. Info. Theory*, **18**, pp. 825–826 (1972).
44. van Lint, J. H.: A survey of perfect codes. *Rocky Mountain J. Math.*, **5**, pp. 199–224 (1975).
45. van Lint, J. H. and MacWilliams, F. J.: Generalized quadratic residue codes. *IEEE Trans. Info. Theory*, **24**, pp. 730–737 (1978).
46. MacWilliams, F. J. and Sloane, N. J. A.: *The Theory of Error-correcting Codes*. Amsterdam–New York–Oxford: North Holland, 1977
47. Massey, J. L.: *Threshold Decoding*. Cambridge, Mass.: MIT Press, 1963.

48. Massey, J. L. and Garcia, O. N.: Error-correcting codes in computer arithmetic. In: *Advances in Information Systems Science*, Vol. 4, Ch. 5. (Edited by J. T. Ton). New York: Plenum Press, 1972.
49. Massey, J. L., Costello, D. J. and Justesen, J.: Polynomial weights and code construction. *IEEE Trans. Info. Theory*, **19**, pp. 101–110 (1973).
50. McEliece, R. J., Rodemich, E. R., Rumsey, H. C. and Welch, L. R.: New upper bounds on the rate of a code via the Delsarte–MacWilliams inequalities. *IEEE Trans. Info. Theory*, **23**, pp. 157–166 (1977).
51. McEliece, R. J.: *The Theory of Information and Coding.* Encyclopedia of Math. and its Applications, Vol. 3. Reading, Mass.: Addison-Wesley, 1977.
52. McEliece, R. J.: The bounds of Delsarte and Lovasz and their applications to coding theory. In: *Algebraic Coding Theory and Applications.* (Edited by G. Longo, CISM Courses and Lectures, Vol. 258. Wien–New York: Springer, 1979.
53. Peterson, W. W. and Weldon, E. J.: *Error-correcting Codes.* (2nd ed.). Cambridge, Mass.: MIT Press, 1972.
54. Piret, Ph.: Structure and constructions of cyclic convolutional codes. *IEEE Trans. Info. Theory*, **22**, pp. 147–155 (1976).
55. Piret, Ph.: Algebraic properties of convolutional codes with automorphisms. Ph.D. Dissertation. Univ. Catholique de Louvain, 1977.
56. Posner, E. C.: Combinatorial structures in planetary reconnaissance. In: *Error Correcting Codes.* (Edited by H. B. Mann. pp. 15–46. New York–London–Sydney–Toronto: Wiley, 1968.
57. Preparata, F. P.: A class of optimum nonlinear double-error-correcting codes. *Info. and Control*, **13**, pp. 378–400 (1968).
58. Rao, T. R. N.: *Error Coding for Arithmetic Processors.* New York–London: Academic Press, 1974.
59. Roos, C.: On the structure of convolutional and cyclic convolutional codes. *IEEE Trans. Info. Theory*, **25**, pp. 676–683 (1979).
60. Schalkwijk, J. P. M., Vinck, A. J. and Post, K. A.: Syndrome decoding of binary rate k/n convolutional codes. *IEEE Trans. Info. Theory*, **24**, pp. 553–562 (1978).
61. Selmer, E. S.: Linear recurrence relations over finite fields. Univ. of Bergen, Norway: Dept. of Math., 1966.
62. Shannon, C. E.: A mathematical theory of communication. *Bell Syst. Tech. J.*, **27**, pp. 379–423, 623–656 (1948).
63. Sidelnikov, V. M.: Upper bounds for the number of points of a binary code with a specified code distance. *Info. and Control*, **28**, pp. 292–303 (1975).
64. Sloane, N. J. A. and Whitehead, D. S.: A new family of single-error-correcting codes. *IEEE Trans. Info. Theory*, **16**, pp. 717–719 (1970).
65. Sloane, N. J. A., Reddy, S. M. and Chen, C. L.: New binary codes. *IEEE Trans. Info. Theory*, **18**, pp. 503–510 (1972).
66. Solomon, G. and van Tilborg, H. C. A.: A connection between block and convolutional codes. *SIAM J. Appl. Math.*, **37**, pp. 358–369 (1979).
67. Szegö, G.: *Orthogonal Polynomials.* Colloquium Publications, Vol. 23. New York: Amer. Math. Soc. (revised edition), 1959.
68. Tietäväinen, A.: On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math.*, **24**, pp. 88–96 (1973).
69. van Tilborg, H. C. A.: Uniformly packed codes. Thesis, Eindhoven Univ. of Technology, 1976.
70. Tricomi, F. G.: *Vorlesungen über Orthogonalreihen.* Grundlehren d. math. Wiss. Band 76. Berlin–Heidelberg–New York: Springer, 1970.
71. Tzeng, K. K. and Zimmerman, K. P.: On extending Goppa codes to cyclic codes. *IEEE Trans. Info. Theory*, **21**, pp. 712–716 (1975).

汉英名词索引

二　画

三　画

四　画

五　画

六　画

七　画

八　画

九 画

十 画

十 一 画

十 二 画

十三画—十八画

其 它

英汉名词索引